Product Guide

McAfee ePO Deep Command 2.1.0

For use with ePolicy Orchestrator 4.6.x, 5.x.x Software

COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1 Introduction 7

Product features . . . 7
Intel AMT overview . . . 9
Product components . . . 10
Getting started . . . 13
Setting up your environment . . . 13
Architecture and how components communicate . . . 14

2 Installation 17

Requirements . . . 18
System requirements . . . 18
Software requirements . . . 19
Operating system requirements . . . 19
Upgrade requirements . . . 20
Supported Intel® AMT versions . . . 20
Required ports . . . 21
ePO Deep Command components in Software Manager . . . 23
Install the software . . . 24
Install or upgrade the ePO Deep Command extensions . . . 24
Deploy the Discovery and Reporting plug-in . . . 25
Assign the AMT tag to systems . . . 25
Deploy the Management Framework client . . . 26
Modify ePO Deep Command settings . . . 26
Configure user permissions . . . 28
Manage certificates . . . 30
Export an active certificate . . . 30
Import a certificate . . . 30
Regenerate certificates . . . 30
Uninstall the software . . . 31
Uninstall the RCS Management plug-in . . . 31
Uninstall the ePO Deep Command client . . . 32
Uninstall the Discovery and Reporting plug-in . . . 32
Remove the ePO Deep Command extensions . . . 32

3 Basics of Intel AMT configuration 35

Host-based configuration . . . 36
Client Control mode . . . 36
User consent requirement . . . 37
Host-based configuration authentication . . . 38
Remote configuration . . . 38
Admin Control mode . . . 38
How RCS Manager plug-in works . . . 40
Remote configuration authentication . . . 40
Configuration states . . . 42

4 Configuring Intel AMT systems 43

Synchronize with Windows Active Directory . . . 43
Register Windows Active Directory server . . . 43
Schedule LDAP synchronization . . . 44
Set Intel AMT configuration preferences . . . 44
Import a configuration profile template . . . 45
Create a configuration profile . . . 45
Set Intel AMT credentials . . . 48
Perform host-based configuration . . . 49
Perform remote configuration . . . 50
Prerequisites for remote configuration . . . 50
Enable McAfee ePO Deep Command certificates support in Intel RCS . . . 51
Install the Profile Manager extension . . . 51
Check in the RCS Manager package . . . 51
Deploy the RCS Manager plug-in . . . 52
Configure Intel AMT systems using remote configuration policy . . . 53
Test your connection to an Intel AMT system . . . 54
Unconfigure Intel AMT systems through McAfee ePO . . . 54
Unconfigure Intel® AMT systems using policy . . . 55
Identify unconfigured systems . . . 55
Clear the AMT tag . . . 56

5 Setting up your environment for Remote Access 57

Install the ePO Deep Command Gateway server . . . 58
Generate certificates for Stunnel . . . 59
Add DH parameter to the .pem file . . . 60
Configure Stunnel . . . 60
Validate certificate . . . 61

6 Enabling Intel AMT wireless manageability 63

Prerequisites for using wireless with ePO Deep Command . . . 64
Wireless profiles . . . 64
Wireless profile synchronization . . . 64
Create a delta configuration profile for wireless . . . 65
Validate wireless settings . . . 67

7 Reporting on your Intel AMT systems 69

Queries and reports . . . 69
Predefined reporting queries . . . 69
Predefined RCS management queries . . . 71
Predefined management queries . . . 71
View default queries . . . 71
Custom query filters . . . 72
Dashboards and monitors . . . 75
Discovery and Reporting Summary dashboard . . . 75
Management Summary dashboard . . . 80
RCS Management Summary dashboard . . . 81
Readiness Summary dashboard . . . 81
Benefits Summary dashboard . . . 82
ePO Deep Command system properties . . . 85
Discovery and Reporting plug-in properties . . . 85
Management Framework client properties . . . 91
RCS Management plug-in properties . . . 92

8 Managing your Intel AMT systems 93

Using policies to manage Intel AMT systems . . . 93

Create the Intel AMT configuration policies . . . 94
Create the Intel AMT policies . . . 96
Creating the Client Task Execution policy . . . 101
Compare ePO Deep Command policies . . . 102
Create the Profile Manager policies . . . 103
Create a Configuration Profile policy . . . 103
Set the time-out for remote system . . . 105
Use the Intel AMT actions . . . 105
Turn on your systems . . . 106
Obtain User Consent . . . 107
Boot or restart to BIOS . . . 107
Boot or restart a system normally . . . 108
Connect to a system using the Serial-over-LAN . . . 109
Boot or restart using IDE-Redirection . . . 109
Stop image redirection . . . 111
Enforce Intel AMT configuration policy . . . 111
Enforce Intel AMT policies . . . 111
Automate Intel AMT policy enforcement . . . 112
Schedule and enforce out-of-band AMT policies . . . 112
Schedule out-of-band power on . . . 112
Maintenance tasks . . . 113
Schedule a maintenance task . . . 114
Compare maintenance tasks . . . 114
Managing events and logs . . . 115
ePO Deep Command events . . . 115
ePO Deep Command logs . . . 117

9 Connecting to Intel AMT systems using KVM 119
KVM Viewer overview . . . 120
KVM requirements . . . 121
Download McAfee KVM Viewer . . . 121
Set up the client for KVM . . . 121
Add McAfee root CA certificate . . . 122
Place the certificate manually . . . 122
Import the certificate in KVM console . . . 122
Use Microsoft Management Console . . . 123
Modify the McAfee KVM Viewer settings . . . 123
Connect to a local system . . . 126
Connect to a remote system . . . 126
Switch the connection to a different system . . . 126
McAfee KVM Viewer options . . . 127

10 Troubleshooting 129

11 Frequently asked questions 141

A Additional information 145
Create a configuration profile using Intel RCS . . . 145
Customize wireless retry settings . . . 149
Set up the environment for Microsoft CA authentication . . . 150
Import certificates to server . . . 151
Create a certificate chain . . . 151
Import certificates to McAfee ePO . . . 152
Create a certificate template . . . 152
Enable the certificate template . . . 154
Issue certificates automatically . . . 154

Create a configuration profile that uses Microsoft CA certificates 154
Generate certificates for Stunnel using Microsoft CA 156
Intel® MEBX password format 157
Validate permissions 157
Modify WMI permissions to add domain computers 157
Modify DCOM permissions to add domain computers 159
Self-signed configuration certificates 160
Intel® AMT action logs 161
Python scripts for ePO Deep Command 162
Download the python client 162
Sample script for the *Power On* action 162
Sample script for Intel AMT policy enforcement 163

Index **165**

1 Introduction

McAfee ePO Deep Command provides centralized control to your Intel® Active Management Technology (AMT) systems regardless of whether they are powered on, or if an operating system is installed or working.

The ePO Deep Command software integrates the management and automation features of McAfee® ePolicy Orchestrator® (McAfee ePO™) with the hardware-based security and manageability features of Intel® AMT. The Intel® AMT feature is included on your systems equipped with Intel® vPro™. Use ePO Deep Command to configure Intel® AMT firmware, perform Intel® AMT actions, and troubleshoot any issues.

Contents

- *Product features*
- *Intel AMT overview*
- *Product components*
- *Getting started*

Product features

The ePO Deep Command features help configure, manage, and report on your Intel® AMT systems.

Feature	Description
Discovery and Reporting	Retrieve the Intel® AMT and BIOS properties from managed systems, then view reports to analyze your Intel® AMT infrastructure. This feature requires the Discovery and Reporting software.
Dashboards and monitors	Find information using the dashboard monitors for the installed ePO Deep Command components: • Which managed systems are Intel® AMT-equipped • Which Intel® AMT systems were configured using the RCS Manager plug-in. • Which profile was used to configure the Intel® AMT systems • Which systems meet host-based configuration requirements. • Which systems meet remote configuration requirements • Which systems have a particular Intel® AMT feature enabled • Which version of Intel® AMT firmware is installed on a system • What's the configuration status of Intel® AMT systems

Feature	Description
Intel® AMT firmware configuration	Use ePO Deep Command to perform host-based configuration or remote configuration on your Intel® AMT systems: • Host-based configuration is initiated by enforcing a configuration policy that uses the host-based configuration profile. • Remote configuration requires the RCS Manager plug-in, which directly communicates with your managed Intel® RCS server, and a remote configuration policy.
Intel® AMT system management	Enforce the required in-band and out-of-band policies to the Intel® AMT systems. This feature requires the Management Framework software.

Intel® AMT actions	Perform these actions on your Intel® AMT systems:
	• Power on Intel® AMT systems.
	• Use Serial-over-LAN (SOL) to redirect the input and output of the serial port of the Intel® AMT systems over Internet Protocol (IP address).
	• Boot or restart a system.
	• Boot or restart using IDE-Redirection.
	• Boot or restart to BIOS.
	• Configure Intel® AMT firmware.
	• Stop Image Redirection.
	• Obtain user consent.
	This feature requires the Management Framework software.
	The Graceful shutdown feature in Intel® AMT 9.x allows you to turn off your Intel® AMT systems gracefully when:
	• Intel® AMT version is 9.x
	• Either of these Intel® AMT actions are performed:
	  • **Normal Boot/Reboot**
	  • **Boot/Reboot to BIOS Setup**
	  • **Boot/Reboot from Image (IDE-R)**
	• A user session is active on the Intel® AMT system.

Client Initiated Local Access (CILA)	Enable the local Intel® AMT systems to initiate a call for technical assistance to McAfee ePO from their BIOS or operating system. This feature requires the Management Framework software.
Client Initiated Remote Access (CIRA)	Enable the Intel® AMT systems that are outside the enterprise to initiate a call for technical assistance to McAfee ePO from their BIOS or the operating system. This feature requires the Management Framework software and Gateway server.
Remote Keyboard-Video-Mouse (KVM)	Remotely access and troubleshoot your Intel® AMT systems. This feature requires McAfee KVM Viewer software).

Feature	Description
Maintenance tasks	Configure these maintenance tasks: • Synchronize Intel® AMT time • Synchronize network settings • Reissue Intel® AMT certificates • Renew Active Directory password • Renew Intel® AMT admin password This feature requires the Management Framework software.
McAfee Endpoint Encryption integration	Enable Intel® Active Management Technology features on the McAfee Endpoint Encryption secured systems. This action protects the Intel® AMT systems from unauthorized access, loss, and exposure of data. For configuration information, see *McAfee Endpoint Encryption out-of-band management* in *McAfee Endpoint Encryption for PC Product Guide*.
Queries and reports	Generate reports comprised of charts and tables by creating custom queries or executing the predefined queries for the installed ePO Deep Command components.

Intel AMT overview

Intel® AMT is a hardware-based technology for remotely managing and securing systems using out-of-band communication.

With out-of-band communication, administrators can access Intel® AMT systems when systems are turned off.

An Intel® AMT-equipped system has these qualities:

- Intel® AMT is part of the Intel® Management Engine, which is built into systems with Intel® vPro™ technology and includes a separate processor.
- You can perform basic system management tasks on a system, even when it has a crashed hard drive or if it's turned off.
- Its hardware-based remote management, security management, power management, and remote configuration features allow you to access it from remote locations.
- It relies on a hardware-based out-of-band communication channel that operates below the operating system level.
- The communication channel does not depend on:
  - State of the operating system: present, corrupt, down, encrypted, crashed, or missing.
  - Power state of the system: powered on or off.
  - Presence of a management agent.
  - State of many hardware components such as hard disk drives.

Using ePO Deep Command, you can manage client systems that have:

- Intel® AMT-enabled chipset
- Network hardware and software
- Corporate network connection (with an AC power source)

Setting up the environment requires that you configure your Intel® AMT firmware with certificates and integrate ePO Deep Command into the existing security framework.

When an Intel® AMT system is configured to use Wi-Fi, ePO Deep Command allows out-of-band communication to clients in a wireless environment.

Product components

The ePO Deep Command software is comprised of four modules: Discovery and Reporting, Management Framework, Profile Manager, and KVM Viewer.

Discovery and Reporting module

The ePO Deep Command Discovery and Reporting module collects detailed information about your network systems that are equipped with Intel® AMT. This module adds these items to McAfee ePO:

- **Discovery plug-in** — This plug-in detects Intel® AMT and BIOS properties of managed systems in your network. The data collected is displayed on the dashboard. The plug-in is added automatically to master repository during installation, and can be deployed to client systems using the predefined deployment task.
- **Discovery and Reporting plug-in deployment task** — This predefined deployment task is added to the **Client Task Catalog**. You can deploy it to the managed systems you select.
- **Reporting query group** — These predefined queries collect important details about the Intel® AMT-equipped systems in your network. These queries retrieve and display information about Intel® vPro™ and their BIOS properties. You can modify these queries, or create custom queries.
- **Discovery and Reporting dashboard** — This dashboard displays a collection of monitors based on the default ePO Deep Command Reporting query results. All Intel® AMT and BIOS properties of managed systems are displayed in one place.
- **Readiness Summary dashboard** — This dashboard include monitors that display the count of Intel® AMT systems that meet and do not meet the requirements for remote configuration and host-based configuration.
- **AMT tag** — This tag is automatically assigned to managed systems that are fully configured for Intel® AMT functionality.
- **Run Tag Criteria task** — The predefined task evaluates each system against the AMT tag criteria (advisable to run every time you configure or unconfigure client systems).

Management Framework module

The ePO Deep Command Management Framework module delivers "beyond-the-operating system" security management. This feature enables administrators to perform tasks such as to turn on systems, execute security tasks, and return the Intel® AMT systems to their previous power state. This component is required for performing Intel® AMT actions and Intel® AMT configuration. This module adds these items to McAfee ePO console:

- **Management client** — This plug-in manages the core functionality to run client tasks, enforce policies, and generate events. It is added to master repository when the software is installed, and can be deployed to client systems using the predefined deployment task.
- **Management client deployment task** — This predefined deployment task is added to the **Client Task Catalog**. You can deploy it to the managed systems you select.
- **Management queries** — These predefined queries retrieve information from Intel® AMT systems that are managed by ePO Deep Command. You can modify these queries, or create custom queries.
- **Management Summary dashboard** — This dashboard displays a collection of monitors based on the results of the default ePO Deep Command Management queries.
- **AMT actions** — This action group lists the ePO Deep Command actions that can be performed on managed Intel® AMT systems. These actions help you configure, unconfigure, manage, and enforce policies to your Intel® AMT-equipped client systems.
- **AMT policies** — This category in the **Policy Catalog** includes options to create and assign policies for using Intel® AMT features such as Alarm Clock, Client Initiated Local Access, Client Initiated Remote Access, and KVM.
- **Client Task Execution** — This category in the **Policy Catalog** includes options to create and assign policies for executing the Intel® AMT client-side actions such as running the arbitrary command and parameters when turned on using the *Power on* action or the scheduled Alarm Clock.
- **AMT configuration policies** — This category in the **Policy Catalog** includes options to create and assign policies for configuring or unconfiguring Intel® AMT systems.
- **Gateway module** — This module is installed on your Agent Handler. It facilitates communication between McAfee ePO and managed Intel® AMT systems outside the enterprise environment (needed for the Client-Initiated Remote Access feature).

Profile Manager module

The ePO Deep Command Profile Manager includes options on how you configure and unconfigure your Intel® AMT systems using the remote configuration through McAfee ePO. This module adds these items to McAfee ePO:

- **RCS Manager plug-in** — This plug-in retrieves configuration profiles from the Intel® RCS servers, and reports back to McAfee ePO. It is added automatically to master repository during installation, and can be deployed to Intel® RCS server systems using the predefined deployment task.
- **RCS Management Summary dashboard** — This dashboard displays a monitor that represents the managed Intel® AMT systems by each Intel® RCS server.
- **RCS Management queries** — These predefined queries retrieve information from the ePO Deep Command managed Intel® RCS servers. You can modify these queries, or create custom queries.
- **Configuration Profile policy** — This policy provides options to create a configuration profile to be used for Intel® AMT configuration.
- **Remote Configuration Service Policies** — This policy allows you to set the timeout for the remote connections.

McAfee KVM Viewer module

Administrators can use the McAfee KVM Viewer module to remotely access Intel® AMT systems that are KVM-enabled and -supported. From the McAfee KVM Viewer console, you can perform actions on the connected Intel® AMT system such as turn it on, turn if off, restart it, and boot it with an IDE-redirection device.

The McAfee KVM Viewer has an external console; however, the Intel® AMT policy can be configured in McAfee ePO with these KVM settings:

- **Enable or disable KVM support** — If KVM is supported on an Intel® AMT system, enable this feature on the client.
- **User consent** — Specify whether to take user consent for KVM connections. If user's consent is enabled, it generates a passcode on the Intel® AMT system screen when an administrator tries to connect. The same passcode must be entered in the KVM console for a successful connection. You can also specify the time after which the passcode expires.
- **Default monitor** — If you are using multiple monitors, select which monitor of the client system to display: **Primary**, **Secondary**, or **Tertiary**. This table lists the maximum screen resolution supported for an Intel® AMT system.

Client	Screen resolution (with 16-bits of color depth)
Intel® AMT 6.0	1600x1200
Intel® AMT 6.0 maintenance release 2	1920x1080
Intel® AMT 7.x	1920x1200
Intel® Management Engine 8.0	1920x1200

- **Session timeout** — Specify the time after which the KVM connection must time out.

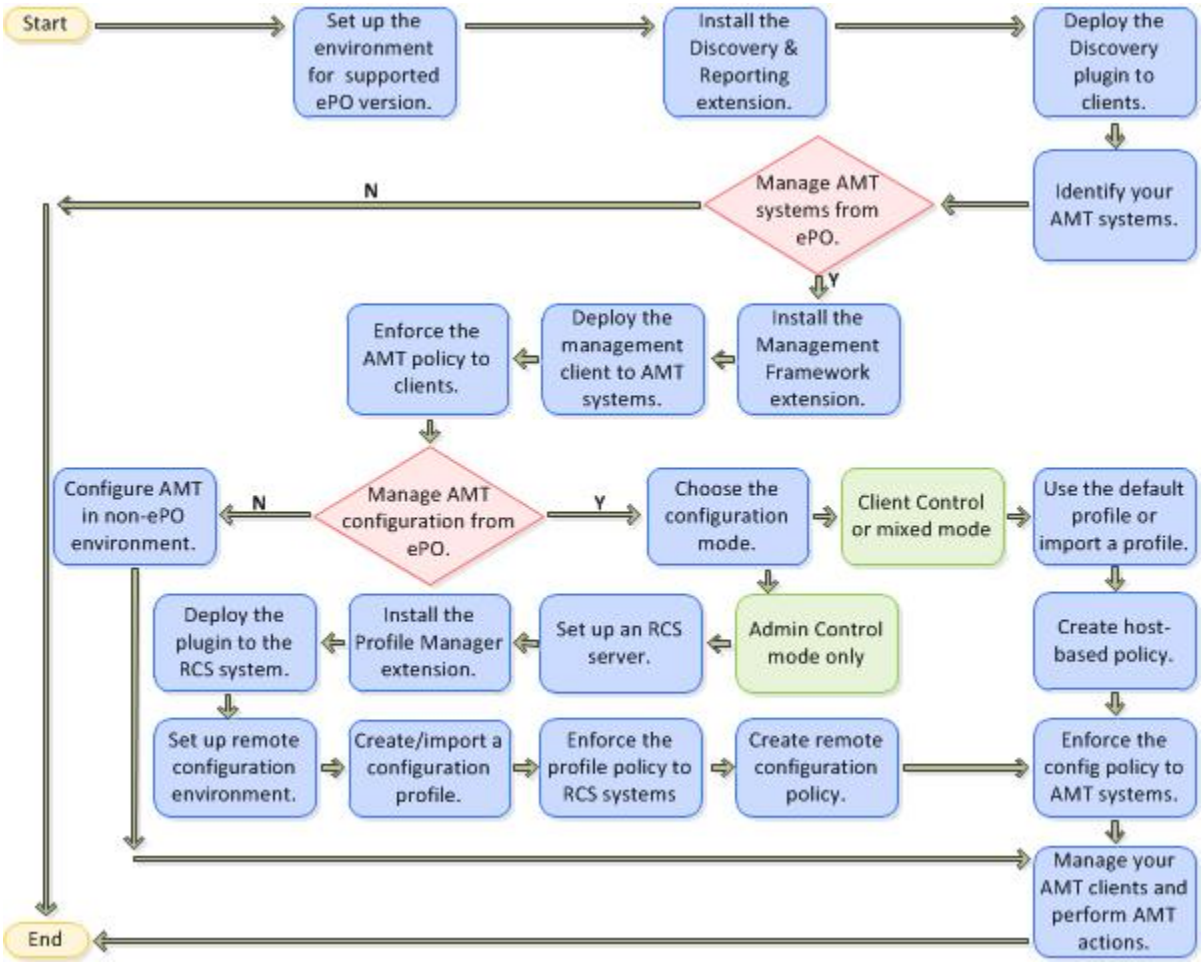
Getting started

Before using ePO Deep Command, make sure that you have specific software, hardware, and network configurations in place.

Setting up your environment

Installing ePO Deep Command Discovery and Reporting software is your first step, then you set up other modules, as required.

This diagram illustrates the actions required to set up your software.


Start
Set up the environment for supported ePO version.
Install the Discovery & Reporting extension.
Deploy the Discovery plugin to clients.
Identify your AMT systems.
Manage AMT systems from ePO.
N
Y
Install the Management Framework extension.
Deploy the management client to AMT systems.
Enforce the AMT policy to clients.
Manage AMT configuration from ePO.
N
Y
Configure AMT in non-ePO environment.
Choose the configuration mode.
Client Control or mixed mode
Use the default profile or import a profile.
Admin Control mode only
Set up an RCS server.
Install the Profile Manager extension.
Deploy the plugin to the RCS system.
Create host-based policy.
Create remote configuration policy.
Enforce the profile policy to RCS systems
Create/import a configuration profile.
Set up remote configuration environment.
Enforce the config policy to AMT systems.
Manage your AMT clients and perform AMT actions.
End

For more information on the Intel® AMT configuration process, see *Preparing your Intel AMT systems*. For detailed instructions on each action, see *Installation and configuration*.

See also

Installation on page 3
Basics of Intel AMT configuration on page 3

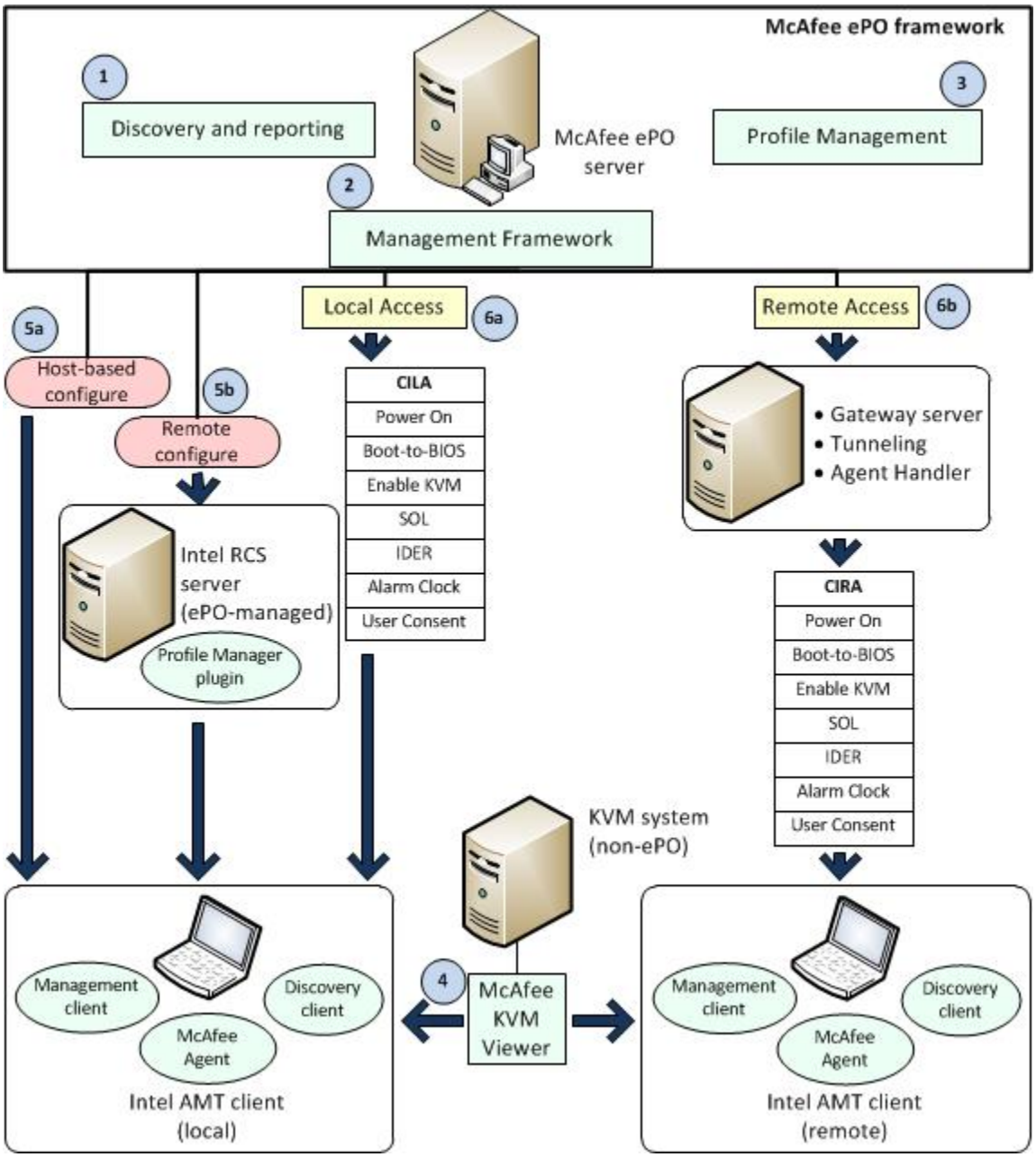
Architecture and how components communicate

ePO Deep Command is comprised of multiple modules, which help you identify, manage, configure, and troubleshoot your Intel® AMT systems.

When installed on McAfee ePO, these modules work with your Intel® AMT systems to deliver greater control of your secure environment.

- Discovery and Reporting module
- Management Framework module
- Profile Manager module
- McAfee Keyboard-Video-Mouse (KVM) Viewer module

High-level architecture



Step	Details	
1	Discovery and Reporting plug-in is installed on McAfee ePO, then deployed to client systems. This plug-in detects the Intel® AMT systems in your organization.	
2	Management client software is installed on McAfee ePO, then deployed to client systems. This plug-in allows you to perform actions and enforce other policies on your Intel® AMT systems.	
3	Profile Management software is required for Intel® AMT configuration. It includes:	
	Profile Management extension	Adds **Configuration Profile** policy to create a configuration profile for Intel® AMT configuration.
	RCS Manager plug-in	Deploys on managed Intel® RCS server and needed only for remote configuration. It retrieves the configuration profiles and other settings that are required for the configuration.
4	KVM Viewer software can be installed on an unmanaged system. However, Intel® AMT systems must be KVM-supported and -enabled. You can create and enforce the KVM policy from McAfee ePO. The ePO Deep Command KVM console helps you to access and troubleshoot Intel® AMT systems locally or remotely.	
5	The Management client allows performing AMT actions on Intel® AMT systems. It also facilitates the Intel® AMT configurations using one of these methods:	
	a — Host-based configuration	Uses the host-based configuration profile and settings.
	b — Remote configuration	Uses the configuration settings retrieved by the RCS Management plug-in.
	To allow configuration from McAfee ePO, the Intel® AMT system must be located within the local environment. Use alternate configuration methods for remote clients.	
6	Based on the Intel® AMT system location, the communication workflow differs as follows:	
	a — Local clients	• Management client directly communicates with Intel® AMT systems to configure them, perform Intel® actions, and enforce other policies. • Local Access feature is used. The Local Area Network (LAN) Agent Handler to be used for the Local Access policy must be active.
	b — Remote clients	• Gateway server and tunneling software are installed and configured on the Agent Handler or McAfee ePO. They allow communication between McAfee ePO and remotely managed Intel® AMT systems. • Remote Access feature is used. • Management client performs Intel® AMT actions such as *Power on*, *Serial-over-LAN*, *IDE-Redirection*, and *Boot/Reboot*.

ePO Deep Command components work on McAfee ePO framework. See the McAfee ePO documentation for your version of the software for details on standard features such as server tasks, dashboards, and queries.

2 Installation

Perform a series of tasks to set up your ePO Deep Command software.

1. Make sure that your system meets the requirements.
2. Install the ePO Deep Command Discovery and Reporting extension.
3. Deploy the ePO Deep Command Discovery and Reporting plug-in to the Intel® AMT systems.
4. Generate reports on your client systems to identify the Intel® AMT-enabled systems.
5. Install the ePO Deep Command Management Framework software.
6. Deploy the ePO Deep Command client plug-in to Intel® AMT systems.
7. (Optional) Provide Intel® AMT credentials and import server authentication certificates.
8. Import trusted root CA certificates.
9. (Optional) Install and configure the Profile Manager software to configure Intel® AMT systems through McAfee ePO.
10. Test your connection to the Intel® AMT systems from McAfee ePO.
11. Configure user access permissions.
12. (Optional) Configure your Intel® AMT systems using host-based configuration or remote configuration from McAfee ePO.
13. (Optional) Set up and configure ePO Deep Command Gateway server (required to use the Client Initiated Remote Access feature).

Contents

- *Requirements*
- *ePO Deep Command components in Software Manager*
- *Install the software*
- *Configure user permissions*
- *Manage certificates*
- *Uninstall the software*

Requirements

Verify that your system meets these requirements before you start the installation process.

System requirements

Systems	Requirements
McAfee ePO	• Version 4.6 Patch 6 or later • Version 5.x See the McAfee ePO documentation for system requirements.

Intel® AMT systems (common for both wired and wireless environments)	• **CPU**: Intel® vPro™ as listed in this link:
	http://www.intel.com/support/vpro/sb/CS-030703.htm
	• **RAM**: 512 MB minimum (1 GB recommended)
	• **Hard Disk**: 200 MB minimum free disk space
	• **Intel® AMT version**: 5.x or later
	For McAfee® Endpoint Encryption for PC integration, Intel® AMT version 6.x or later is required. For host-based configuration, Intel® AMT 7.x or later is required. Contact your hardware vendor to obtain the latest drivers and firmware.
	• **Graphics**: Intel® Integrated 3000 or higher (required for McAfee KVM Viewer connection)
	• **Network Interface Card (NIC)**: Onboard (Multiple NICs are not supported.)
	• **Drivers**:
	  • Intel® Management Engine Interface driver
	  • Intel® Local Manageability Service driver (required for host-based configuration)
	Contact your hardware vendor to obtain the latest drivers and firmware.

Intel® AMT systems in wireless environment	• **Wireless Network Card**: Onboard
	• **Driver**: Intel® PROSet.
	Obtain the latest drivers for your version of operating system. Make sure that the system has these minimum supported versions of the wireless software:
	  • **For Windows 7** — Intel® PROSet 15.3.0 or later
	  • **For Windows 8** — Intel® PROSet 15.5.0 or later

Intel® RCS™ server	Version 8.2 or later (required for remote configuration)

Software requirements

Make sure that you have the required software installed for the ePO Deep Command module that you're installing.

Software	Requirements
Discovery and Reporting plug-in	McAfee Agent for Windows on the Intel® AMT systems • Version 4.6.0 Patch 3 or later • Version 4.8.x
Management Framework client	McAfee Agent for Windows on the Intel® AMT systems • Version 4.6.0 Patch 3 or later • Version 4.8.x
RCS Management plug-in	McAfee Agent for Windows on the managed Intel® RCS server • Version 4.6.0 Patch 3 or later • Version 4.8.x
Internet browser	• Internet Explorer 7.0 or later • Mozilla Firefox 3.6.20 or later • Google Chrome 17 or later (only with ePolicy Orchestrator 5.x) Pop-up windows must be allowed.

The Management Framework module requires the Discovery and Reporting module to function correctly.

Operating system requirements

System	Software
McAfee ePO server*	For system requirements, see the McAfee ePO documentation for your version of the software.
Intel® RCS server*	For system requirements, see the Intel® Setup and Configuration Service (Intel® SCS) User Guide for your version of the software.
Intel® AMT systems	• Windows 7 or later (32- or 64-bit) • Windows 8 or later • Windows Server 2008 R2 or later (32- or 64-bit) • Windows Server 2003 or later (32- or 64-bit) • Windows XP with Service Pack 3 (32- or 64-bit)

* If its installed on a Windows Server 2003 and Windows XP system, see these KB articles:

- Microsoft Knowledge Base article # 968730 (http://support.microsoft.com/kb/968730)
- Microsoft Knowledge Base article # 938397 (http://support.microsoft.com/kb/938397)

Upgrade requirements

You can upgrade to ePO Deep Command 2.1.0 from the software version 2.0.0.

Supported Intel® AMT versions

Some features aren't supported on specific versions of Intel® AMT. Review this table to determine which features and versions are supported on Intel® AMT systems.

Use case	Intel® AMT features used	Intel® AMT version					
		4.0	5.1	6.x	7.x	8.x	9.x
On-demand turn on and restart of systems	Power On	Yes	Yes	Yes	Yes	Yes	Yes
Scheduled turn on of systems	Alarm clock	No	Yes	Yes	Yes	Yes	Yes
Scheduled security tasks	Alarm clock	No	Yes	Yes	Yes	Yes	Yes
EEPC 7.0 Fast Password Reset	Remote Access, Local Access, and Serial-over-LAN	No	No	Yes	Yes	Yes	Yes
EEPC 7.0 Remote Unlock	Remote Access, Local Access, and Serial-over-LAN	No	No	Yes	Yes	Yes	Yes
EEPC 7.0 Remote Remediation	IDE-Redirect, Remote Access, Local Access, and Serial-over-LAN	No	No	Yes	Yes	Yes	Yes
EEPC 7.0 Location Aware Pre-Boot	Remote Access, Local Access, and Serial-over-LAN	No	No	Yes	Yes	Yes	Yes
McAfee KVM Viewer‡	KVM	No	No	Yes	Yes	Yes	Yes
Boot to recovery operating system image (.iso file)	IDE-Redirect	Yes	Yes	Yes	Yes	Yes	Yes
Boot to BIOS setup	Boot with options and Serial-over-LAN	Yes	Yes	Yes	Yes	Yes	Yes
Support for Internet-Connected Systems using McAfee Remote Access	Remote Access	No	Yes	Yes	Yes	Yes	Yes
User Request for Assistance	Remote Access and Local Access	Yes	Yes	Yes	Yes	Yes	Yes
Remote configuration from McAfee ePO	Intel® RCS	Yes	Yes	Yes	Yes	Yes	Yes
Host-based configuration from McAfee ePO§	Intel® Local Manageability Service	No	No	No	Yes	Yes	Yes
Graceful shutdown	Power On, Alarm clock, and Boot/reboot with options	No	No	No	No	No	Yes

‡ Requires Intel integrated graphics.

§ Requires Intel® Local Manageability Service driver.

Online resources for more information on Intel® AMT technology

- Intel® vPro™ Technology
- Intel® Active Management Technology (Intel® AMT)
- Download The Latest Intel® AMT Open Source Drivers

Required ports

Make sure that your network security software doesn't block ports and services that are needed for Intel® AMT communications.

Add these ports, services, and processes as exclusions in the security policy settings of your network security software such as firewall or intrusion prevention system.

Services installed on Agent Handler or McAfee ePO

Service	Feature	Ports	Description
ServiceAMT.exe	Intel® AMT policy enforcement	• 16993 (Policy configuration and remote management features) • 16995 (Redirection over TLS for IDE-Redirection, Serial-over-LAN, and KVM)	This service loads the required plug-in and performs the out-of-band actions on the client.
AMTGatewayService.exe	Remote Access	• 11112 (AMTGatewayService listens to this port for Intel® AMT connections. The tunneling proxy also uses it to forward connections from the Intel® AMT systems.) • 1080 (SOCKS proxy for Remote Access) • 8080 (HTTP proxy for Remote Access)	This service acts as a proxy responsible for mediating communication between the Agent Handler and Intel® AMT systems for Remote Access.
Apache.exe	Remote Access	• 1080 (SOCKS proxy for Remote Access) • 8080 (HTTP proxy for Remote Access)	This acts as proxy for SOCKS and HTTP proxy requests needed for Remote Access tunnel.
Stunnel.exe	Remote Access	• 11111 (Stunnel uses this port to send data received from the Intel® AMT systems to the ePO Deep Command Gateway server) • 12345 (This port is the default port that the Intel® AMT platform uses to connect to the Gateway server.) • 16993 (Policy configuration and remote management features) • 16995 (Redirection over TLS for IDE-Redirection, Serial-over-LAN, and KVM)	This service acts as the SSL tunneling proxy between the Agent Handler and Intel® AMT systems for Remote Access.

Services installed on managed Intel® AMT systems

Service/process	Feature	Ports	Description
AMTMgmtService.exe	Remote configuration	135	This process configures the Intel® client system. Additionally, it's also required for client tasks, property collection, and other policies enforcement.
ACUConfig.exe	Remote configuration	135	This process facilitates configuration or unconfiguration of Intel® AMT systems.
LMS.exe	Host-based configuration	Not applicable	This service is required for host-based configuration.
AMTCT.exe	Client Task Execution	Not applicable	This service executes client tasks.

Services installed on managed Intel® RCS server

Service	Feature	Ports	Description
RCSServer.exe	Remote configuration	135	This service performs remote configuration of Intel® AMT systems.
AMTRCSMgmtService.exe	Remote configuration	Not applicable	This service also deploys MediationCA.dll on the Intel® RCS server and inserts the required certificates for configuration. Collecting properties and enforcing policy on Intel® RCS server
MediationCOMWrapper.exe	Remote configuration	Not applicable	Intel® RCS service for third-party CA certificate.

Other ePO Deep Command services or processes

Service/process	Feature	Ports	Description
MKVMView.exe	McAfee KVM Viewer connection	• 16993 (Policy configuration and remote management features) • 16995 (Redirection over TLS for IDE-Redirection and KVM) • 1080 (SOCKS proxy for Remote Access to McAfee Gateway Server for Remote Access) • 8080 (HTTP proxy for Remote Access to ePO Deep Command Gateway server for Remote Access)	This service allows a connection to an Intel® AMT system remotely to access its Keyboard, Video, and Mouse.
Web interface: *https:/< FQDN of the Intel® AMT system>:16993*	Intel® AMT remote management	16993	This service is required for accessing Intel® AMT from the web interface.

ePO Deep Command components in Software Manager

Here are the components that you see in **Software Manager**, when you select ePO Deep Command from the product list.

Component	Description
Discovery and Reporting extension	Enables the Discovery and Reporting feature on the server. Check in the extension or download to check it in later.
Discovery and Reporting plug-in	Deploys the Discovery and Reporting plug-in to the Intel® AMT systems. Check in the package or download to check it in later.
Management Framework extension	Enables the Management Framework feature on the server. Check in the extension or download to check it in later.
Management Framework client	Deploys the Management Framework plug-in to the Intel® AMT systems. Check in the package or download to check it in later.
Profile Manager extension	Allows the Intel® AMT configuration through the server. Check in the extension or download to check it in later.
RCS Manager	Deploys the RCS Manager plug-in to the managed Intel® RCS server. Check in the package or download to check it in later.
Intel® Setup and Configuration Service software	Sets up environment to configure Intel® AMT systems. Download the software, then install it on the system required.
Gateway server	Sets up environment to enable communication with the remotely managed Intel® AMT system. Download the software, then install it on a server in your corporate DMZ where the Agent Handler is installed.
KVM Viewer	Remotely connects to Intel® AMT systems and allows access to their keyboard, video, and mouse. Download the software, then install it on the system required.
Product guide	The product documentation you can download.
Release notes	The product release information you can download.
Help extension	The product Help extension you can download and install to McAfee ePO to enable assistance in the interface. Once the McAfee ePO Help is installed, click **?** to view definitions of the interface options.

Install the software

Install the extensions and deploy them to manage your Intel® AMT systems.

Tasks

- *Install or upgrade the ePO Deep Command extensions* on page 24
  You can install the required ePO Deep Command software components on McAfee ePO.
- *Deploy the Discovery and Reporting plug-in* on page 25
  Deploy the Discovery and Reporting plug-in to Intel® AMT systems.
- *Assign the AMT tag to systems* on page 25
  Run the predefined **ePO Deep Command: Run Tag Criteria** task to evaluate each system against AMT tag criteria and assign the AMT tag to all configured Intel® AMT systems.
- *Deploy the Management Framework client* on page 26
  Deploy the Management Framework client to your Intel® AMT systems to manage them using Intel® AMT actions, policies, server tasks, and queries.
- *Modify ePO Deep Command settings* on page 26
  Specify ePO Deep Command credentials and import the Server Authentication Certificate in McAfee ePO.

Install or upgrade the ePO Deep Command extensions

You can install the required ePO Deep Command software components on McAfee ePO.

Software Manager provides a single location within McAfee ePO console to review and obtain McAfee software and components. If you already have an earlier version of the software installed, follow this task to upgrade McAfee ePO Deep Command to version 2.1.0.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.

2 On the **Software Manager** page under **Product Categories**, click **Software Not Checked In** | **Licensed**.

3 Select **McAfee ePO Deep Command 2.1** from the product list, then perform one of these:

- For a new installation, select the product components to be installed or select **Check In All**.

  The ePO Deep Command 2.1 extensions contain the associated client-side component package. We recommend that you check in components individually. When you use **Check In All**, duplicate entries of the ePO Deep Command packages are checked in to the **Current** branch in the master repository.

- For upgrade, click **Check In All** to check in all new components, then click **Update All** to update all existing components.

  We recommend that you move previous versions of ePO Deep Command packages to the **Previous** branch before checking in ePO Deep Command 2.1 components. We also recommend that you use **Update All** when previous versions of ePO Deep Command packages exist in the master repository.

  See *Components in Software Manager* for the list of ePO Deep Command components.

4 On the **Check In Software Summary** page, review and accept the End User License Agreement (EULA), then click **OK** to complete the installation.

The checked-in packages appear under **Menu** | **Software** | **Master Repository**. The checked-in extensions appear under **Menu** | **Software** | **Extensions**.

Deploy the Discovery and Reporting plug-in

Deploy the Discovery and Reporting plug-in to Intel® AMT systems.

> **Before you begin**
>
> Make sure that the plug-in package is checked in and listed under **Menu** | **Software** | **Master Repository**.

The **Deploy ePO Deep Command Discovery and Reporting Plugin** client task is created automatically when the ePO Deep Command Discovery and Reporting plug-in is installed on McAfee ePO.

Assign the client task to the selected client computers.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **Product Deployment** under **McAfee Agent**.
2. Click **Assign** in the **Deploy ePO Deep Command Discovery and Reporting Plugin** actions column.
3. Select the required system group where you want to deploy the plug-in, then click **OK** to open the **Client Task Assignment Builder** wizard.
4. On the **Select Task** page, verify the product name, task type, and task name to deploy the product. Next to **Tags**, select one of these as needed, then click **Next**.
   - **Send this task to all computers**
   - **Send this task to only computers that have the following criteria** — Click an appropriate link to configure the criteria.
5. On the **Schedule** page in **Select type**, select **Run immediately**, then click **Next**.
6. Review the summary, then click **Save** to open the **System Tree**.
7. Select the systems or groups where you assigned the task, then click **Actions** | **Agent** | **Wake Up Agents**.
8. Select **Force complete policy and task update**, then click **OK**.

On successful execution, the ePO Deep Command Discovery and Reporting plug-in is deployed to the selected group. To check the task status, navigate to **Server Task Log**.

Assign the AMT tag to systems

Run the predefined **ePO Deep Command: Run Tag Criteria** task to evaluate each system against AMT tag criteria and assign the AMT tag to all configured Intel® AMT systems.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Automation** | **Server Tasks**.
2. Click **Run** for the **ePO Deep Command: Run Tag Criteria**.

On successful execution, the **AMT** tag is assigned to all configured Intel® AMT systems. To check the task status, navigate to **Server Task Log**.

Deploy the Management Framework client

Deploy the Management Framework client to your Intel® AMT systems to manage them using Intel® AMT actions, policies, server tasks, and queries.

> **Before you begin**
>
> Make sure that the ePO Deep Command Management Framework client package is checked in and listed under **Menu** | **Software** | **Master Repository**.

The **Deploy ePO Deep Command Client** task is created automatically when the ePO Deep Command Management Framework client is installed on McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **Product Deployment** under **McAfee Agent**.
2. Click **Assign** in **Deploy ePO Deep Command Client**.
3. Select the required systems or groups where you want to deploy Management Framework, then click **OK**.
4. Click **Next** to schedule the deployment task as needed.
5. Click **Next**, then click **Save**.
6. Send an agent wake-up call.

On successful execution, the ePO Deep Command Management Framework client is deployed to the selected client systems. To check the task status, navigate to **Server Task Log**.

Modify ePO Deep Command settings

Specify ePO Deep Command credentials and import the Server Authentication Certificate in McAfee ePO.

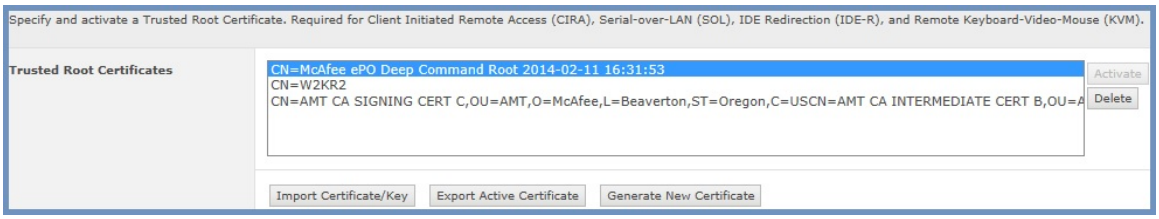
The credentials you specify must be the same as the configuration profile credentials. This procedure authenticates your administrator rights to manage Intel® AMT systems using ePO Deep Command.

Task

For option definitions, click **?** in the interface.

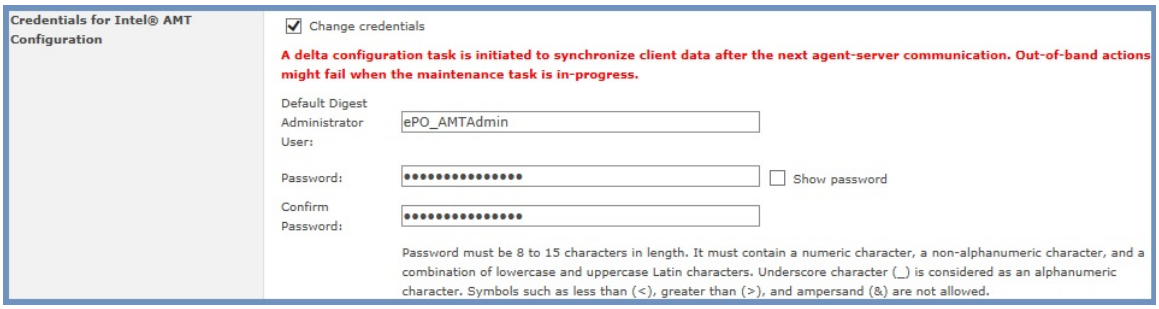
1. In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.
2. In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit** to specify your Intel® AMT credentials and trusted root certificates.

3 In **Trusted Root Certificates**, a pre-activated McAfee ePO Deep Command Root CA (**CN=McAfee ePO Deep Command Root <Date and time>**) is listed. If you have imported a certificate or generated a new McAfee ePO Deep Command Root CA, select it, then click **Activate**. To remove a certificate, select it and click **Delete**.


Specify and activate a Trusted Root Certificate. Required for Client Initiated Remote Access (CIRA), Serial-over-LAN (SOL), IDE Redirection (IDE-R), and Remote Keyboard-Video-Mouse (KVM).
Trusted Root Certificates
CN=McAfee ePO Deep Command Root 2014-02-11 16:31:53
CN=W2KR2
CN=AMT CA SIGNING CERT C,OU=AMT,O=McAfee,L=Beaverton,ST=Oregon,C=USCN=AMT CA INTERMEDIATE CERT B,OU=A
Activate
Delete
Import Certificate/Key
Export Active Certificate
Generate New Certificate

We recommend that you use certificates generated by McAfee ePO Deep Command Root CA. However, if you use Microsoft CA for your environment, click **Import Certificate/Key**. See *Import Microsoft CA certificates* for detailed instructions.

4 In **Credentials for Intel® AMT configuration**, select **Change credentials**, then type the digest user name and password. Click **Show password** to view the password.


Credentials for Intel® AMT Configuration
Change credentials
A delta configuration task is initiated to synchronize client data after the next agent-server communication. Out-of-band actions might fail when the maintenance task is in-progress.
Default Digest Administrator User:
ePO_AMTAdmin
Password:
Show password
Confirm Password:
Password must be 8 to 15 characters in length. It must contain a numeric character, a non-alphanumeric character, and a combination of lowercase and uppercase Latin characters. Underscore character (_) is considered as an alphanumeric character. Symbols such as less than (<), greater than (>), and ampersand (&) are not allowed.

The credentials provided are used for Intel® AMT configuration by default. The default digest admin user name is *ePO_AMTAdmin* and password is randomly generated. For the configuration profiles created in Intel® SCS, make sure that the credentials specified here match with the credentials specified in the Intel® SCS profiles.

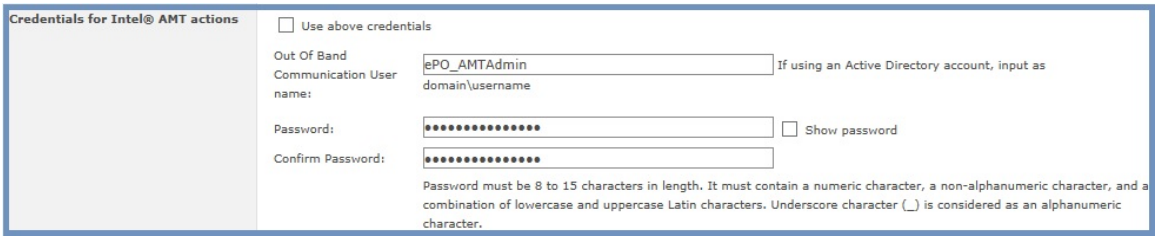
If you create a password, it must:

- Be 8–15 characters in length.
- Contain a numeric character.
- Contain lowercase and uppercase Latin characters.
- Contain a non-alphanumeric character; except "<" (less than), ">" (greater than), and "&" (ampersand) symbols.

Underscore (_) is considered as an alphanumeric character

This updated password is used in all configuration profiles imported in McAfee ePO after the next agent wake-up call to the Intel® RCS system that was used for creating the profiles.

5 In **Credentials for Intel® AMT actions**, select **Change credentials**, then select **Use above credentials**, or type the user name and password. Use `domain\user name` format for Active Directory accounts. Click **Show password** to view the password.


Credentials for Intel® AMT actions
Use above credentials
Out Of Band Communication User name:
ePO_AMTAdmin
If using an Active Directory account, input as domain\username
Password:
Show password
Confirm Password:
Password must be 8 to 15 characters in length. It must contain a numeric character, a non-alphanumeric character, and a combination of lowercase and uppercase Latin characters. Underscore character (_) is considered as an alphanumeric character.

The credentials provided are used for Intel® AMT actions. For a new installation, the default out-of-band communication user name is *ePO_AMTAdmin* and password is randomly generated. For an upgrade, the Intel® AMT credentials that you specified earlier are used by default.

If you create a password, it must meet the requirements listed in step 4.

6 In **CILA/CIRA Event Details**, select the options as needed:

Option	Definition
Disable listening for CILA/CIRA messages on Agent Handlers	Disables *Agent Handlers* to receive incoming local access or remote access calls. It can be used in these situations: • To globally disable local access or remote access without configuring their policy settings. • To disable all other features that depend on them (such as EEPC Unlock).
Extend CIRA/CILA session-opening events to describe the reason they were initiated	Enables *Agent Handlers* to obtain detailed information about the system that initiates a local access or remote access call (such as who initiated the call: EEPC or a user).

7 Click **Save**.

After the next agent-server communication, a maintenance task is initiated to synchronize data between the server, Intel® RCS system, and Intel® AMT systems.

8 On **Threat Event Log** page, look for **Deep Command - Maintenance Success** event to verify the maintenance task completion.

9 Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

See also

Import certificates to server on page 151
Import certificates to McAfee ePO on page 152
Create a configuration profile on page 45

Configure user permissions

Minimum permissions must be set for all users for ePO Deep Command actions, policies, and tasks.

A permission set is a group of permissions granted to a user account for specific products or features of a product. Permission sets can be assigned. For users who are global administrators, all permissions to all products and features are automatically assigned. Global administrators can assign existing permission sets when creating or editing user accounts and when creating or editing permission sets.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **User Management** | **Permission Sets**.

2 Select the permission set where you want to assign ePO Deep Command permissions.

The details appear to the right.

3 Click **Edit** next to the permission set to be modified:

Permission set	Options
ePO Deep Command Actions (added when ePO Deep Command Management Framework is installed)	Grant permissions for these Intel® AMT actions: • **Enforce AMT Policies** — Allows users to enforce Intel® AMT policies on client systems. • **Enforce AMT Firmware Configuration Policy** — Allows users to configure or unconfigure Intel® AMT firmware on the client systems. • **Power On** — Allows users to turn on client systems. • **Boot/Reboot with Options (IDE-R)** — Allows users to restart an Intel® AMT system to a redirected disk. • **Serial-over-LAN Terminal (SOL)** — Allows users to connect to a remote Intel® AMT system through a virtual serial port. • **Get User Consent** — Allows users to connect to generate user consent code for a connection to an Intel® AMT system.
ePO Deep Command Policies (added when ePO Deep Command Management Framework is installed)	Grant permissions for ePO Deep Command policies and tasks: • **No Permissions** — Blocks users from viewing policy and task settings in the ePO Deep Command policies. • **View policy and task settings** — Allows users to view policy and task settings in the ePO Deep Command policies. • **View and change policy and task settings** — Allows users to view and modify the policy and task settings in the ePO Deep Command policies.
ePO Deep Command Profile Manager (added when ePO Deep Command Profile Manager is installed)	Grant permissions for ePO Deep Command configuration policies: • **No Permissions** — Blocks users from viewing policy and task settings in the ePO Deep Command configuration policies. • **View policy and task settings** — Allows users to view policy and task settings in the ePO Deep Command configuration policies. • **View and change policy and task settings** — Allows users to view and modify the policy and task settings in the ePO Deep Command configuration policies.

4 On the **Edit Permissions Set** page for the selected permission set, select the options as needed, then click **Save**.

Manage certificates

Use certificate management options to export a ePO Deep Command root CA certificate for reuse, import it, or regenerate it with the new time stamp, as needed.

Tasks

- *Export an active certificate* on page 30
  You can export an active certificate from McAfee ePO to reuse it.
- *Import a certificate* on page 30
  Import an exported root certificate to McAfee ePO to use it.
- *Regenerate certificates* on page 30
  Generate McAfee ePO Deep Command root CA certificate with the latest time stamp, which can be used to replace a certificate that is expired or removed.

Export an active certificate

You can export an active certificate from McAfee ePO to reuse it.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit**.

3 In **Trusted Root Certificate**, select the certificate to be exported (**CN=McAfee ePO Deep Command Root**) click **Export Active Certificate**, then save the file to your computer.

The file exported is in `.zip` format. Unzip the file to extract the certificates and use them.

Import a certificate

Import an exported root certificate to McAfee ePO to use it.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit**.

3 In **Trusted Root Certificate**, click **Import Certificate/Key**, browse to select a certificate file (.pem, .der, or .p12), enter the certificate file password (for PKCS12 certificates), click **Next**, then click **Save**.

Regenerate certificates

Generate McAfee ePO Deep Command root CA certificate with the latest time stamp, which can be used to replace a certificate that is expired or removed.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit**.

3 For **Trusted Root Certificate**, click **Generate New Certificate**.

A new entry is added for McAfee ePO Deep Command Root in **Trusted Root Certificates**.

4 Select the McAfee ePO Deep Command Root, click **Activate**, then click **OK** to confirm.

5 Reconfigure your Intel® AMT systems to use the updated certificate.

The Intel® AMT actions such as Remote Access, Serial-over-LAN, IDE-Redirection, and KVM access fail if the certificate is not updated on the Intel® AMT.

Uninstall the software

To remove ePO Deep Command from a McAfee ePO server, remove its client components from Intel® AMT systems, then remove the installed extensions.

Tasks

- *Uninstall the RCS Management plug-in* on page 31
  Create a client task to remove the plug-in from Intel® RCS systems, then assign it to the systems.
- *Uninstall the ePO Deep Command client* on page 32
  Create a client task to remove the client from Intel® AMT systems, then assign it to the systems.
- *Uninstall the Discovery and Reporting plug-in* on page 32
  Create a client task to remove the plug-in from Intel® AMT systems, then assign it to the systems.
- *Remove the ePO Deep Command extensions* on page 32
  Remove the ePO Deep Command extensions from the **Software Manager**.

Uninstall the RCS Management plug-in

Create a client task to remove the plug-in from Intel® RCS systems, then assign it to the systems.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **Product Deployment** under **McAfee Agent**.

2 Click **New Task** and select **Product Deployment** to open the **Client Task Catalog: New Task** page.

3 Type a name for the task and any notes, then select appropriate **Target Platforms**.

4 In **Products and components**, select **McAfee ePO Deep Command RCS Manager 2.1.0.xxx**, select **Remove** as the action, select the language, then click **Save**.

5 Click **Save** and exit the **New Task** page.

6 In **Client Task Catalog** under the **Actions** column of your new product deployment task, click **Assign** and select the systems or groups where you want to remove the ePO Deep Command RCS Management plug-in, then click **OK**.

7 Click **Next** to schedule the task as needed, click **Next** again, then click **Save**.

Uninstall the ePO Deep Command client

Create a client task to remove the client from Intel® AMT systems, then assign it to the systems.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **Product Deployment** under **McAfee Agent**.
2. Click **New Task** and select **Product Deployment** to open the **Client Task Catalog: New Task** page.
3. Type a name for the task and any notes, then select appropriate **Target Platforms**.
4. In **Products and components**, select **McAfee ePO Deep Command Client 2.1.0.xxx**, **Remove** as the action, select the language, then click **Save**.
5. Click **Save** and exit the **New Task** page.
6. In **Client Task Catalog** under the **Actions** column of your new product deployment task, click **Assign** and select the systems or groups where you want to remove the ePO Deep Command Management Framework client, then click **OK**.
7. Click **Next** to schedule the task as needed, click **Next** again, then click **Save**.

Uninstall the Discovery and Reporting plug-in

Create a client task to remove the plug-in from Intel® AMT systems, then assign it to the systems.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **Product Deployment** under **McAfee Agent**.
2. Click **New Task** and select **Product Deployment** to open the **Client Task Catalog: New Task** page.
3. Type a name for the task and any notes, then select appropriate **Target Platforms**.
4. In **Products and components**, select **McAfee ePO Deep Command Discovery Plugin 2.1.0.xxx**, select **Remove** as the action, select the language, then click **Save**.
5. Click **Save** and exit the **New Task** page.
6. In **Client Task Catalog** under the **Actions** column of your new product deployment task, click **Assign** and select the systems or groups where you want to remove the ePO Deep Command Discovery and Reporting plug-in, then click **OK**.
7. Click **Next** to schedule the task as needed, click **Next** again, then click **Save**.

Remove the ePO Deep Command extensions

Remove the ePO Deep Command extensions from the **Software Manager**.

You can also remove the ePO Deep Command extensions from the **Extensions** page.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.
2. On the **Software Manager** page under **Product Categories**, click **Checked In Software** | **Licensed**.
3. Select **McAfee ePO Deep Command** from the products list, then click **Remove** next to the extension to be removed. Perform this step for each of the ePO Deep Command extensions checked in to your server.
4. In the **Remove Software Summary** page, click **OK**.

3 Basics of Intel AMT configuration

You must configure your Intel® AMT systems before you can manage them using ePO Deep Command.

You can configure your Intel® AMT firmware from McAfee ePO, or any other external source. With the ePO Deep Command software, you can configure your Intel® AMT systems to Client Control mode using host-based configuration or to Admin Control mode using remote configuration.

The method you choose to configure your Intel® AMT systems depends on many factors such as your network infrastructure, hardware, software, and Intel® AMT features.

For more information on the Intel® AMT configuration process, see the Intel® vPro™ Expert Center website (http://www.intel.com/go/vproexpert).

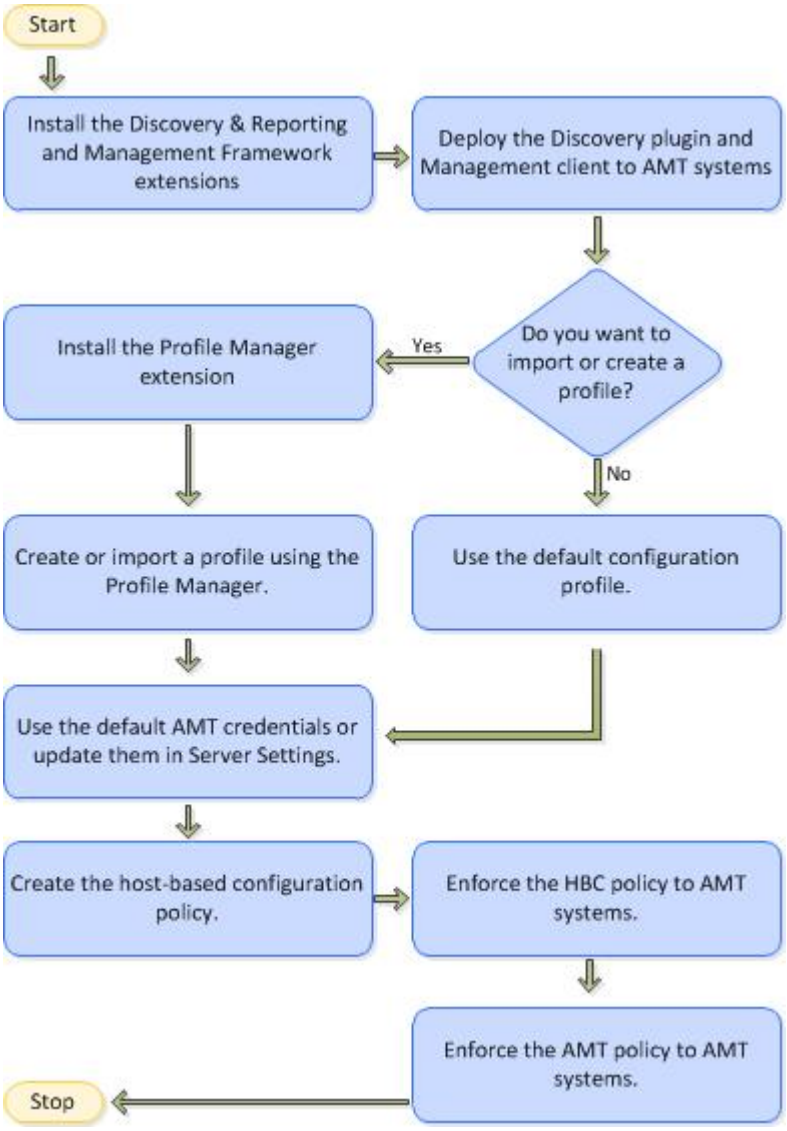
Contents

- *Host-based configuration*
- *Remote configuration*
- *Configuration states*

Host-based configuration

In this method Intel® AMT systems are configured locally using an XML profile containing the required configuration settings.

This diagram presents an overview of the recommended process for configuring systems using the host-based configuration method.


Start
Install the Discovery & Reporting and Management Framework extensions
Deploy the Discovery plugin and Management client to AMT systems
Do you want to import or create a profile?
Yes
Install the Profile Manager extension
No
Create or import a profile using the Profile Manager.
Use the default configuration profile.
Use the default AMT credentials or update them in Server Settings.
Create the host-based configuration policy.
Enforce the HBC policy to AMT systems.
Enforce the AMT policy to AMT systems.
Stop

See also

Perform host-based configuration on page 49

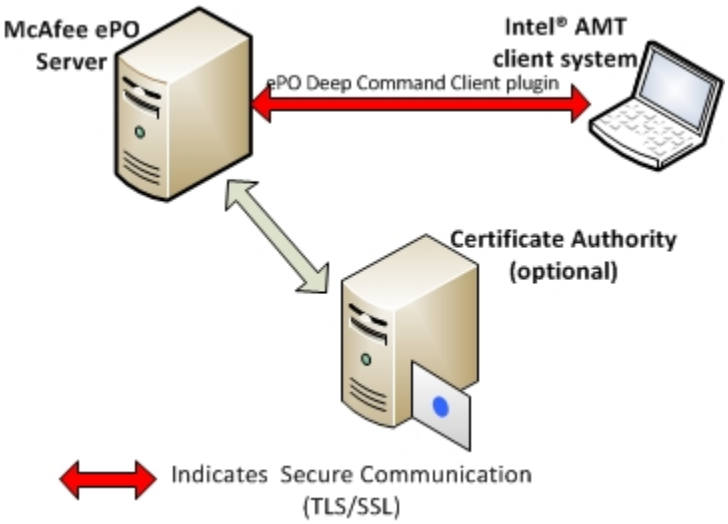
Client Control mode

Intel® AMT systems enter this mode when they are configured using host-based configuration.

Intel® AMT systems in this mode have some security-related limitations such as User Consent being required for certain Intel® AMT actions.

Client Control mode network architecture

This illustration is an overview of a network configuration where your Intel® AMT systems support Client Control mode.



Components in Client Control mode configuration include:

- **McAfee ePO server** — McAfee ePO is the management console from which application and enforcement of Intel® AMT policies are configured and distributed. In the McAfee ePO console:
  - Modify server settings such as selecting or importing required certificates, setting admin credentials to authenticate and enable communication between McAfee ePO and Intel® AMT systems. The Intel® ME BIOS Extension (MEBX) password that you provide is applied to all managed Intel® AMT systems.
  - Create and enforce a configuration policy by selecting the host-based configuration options, which use the host-based configuration profile.
- **Certificate authority server** — McAfee recommends that you use McAfee ePO Deep Command Root CA to simplify the configuration process. However, you can also use an external certificate authority server such as Microsoft CA or a custom root CA. These servers issue certificates to the correct trusted devices within the network. Import these certificates and their private keys to McAfee ePO. You can use Transport Layer Security (TLS) communication by incorporating certificates issued by a CA.

User consent requirement

When user consent is enabled, attempting to initiate a remote connection displays a User Consent Code on the client screen. The administrator must enter this code to gain access.

For devices in Client Control mode (configured using host-based configuration), User Consent mode is required for these actions:

- Boot or restart to BIOS
- Boot using IDE-Redirection (IDE-R)
- KVM Redirection

In Client Control mode, user consent is always required for these actions. In Admin Control mode, it's optional.

Host-based configuration authentication

For host-based configuration, provide credentials for Intel® AMT configuration and use McAfee ePO Deep Command Root CA.

Make sure to configure these settings on the **Server Settings** page:

- **Credentials for Intel® AMT Configuration** — Create a password for your managed Intel® AMT systems. The default user name for Intel® AMT is *admin*.
- **Trusted Root Certificates** — Use McAfee ePO Deep Command Root CA.

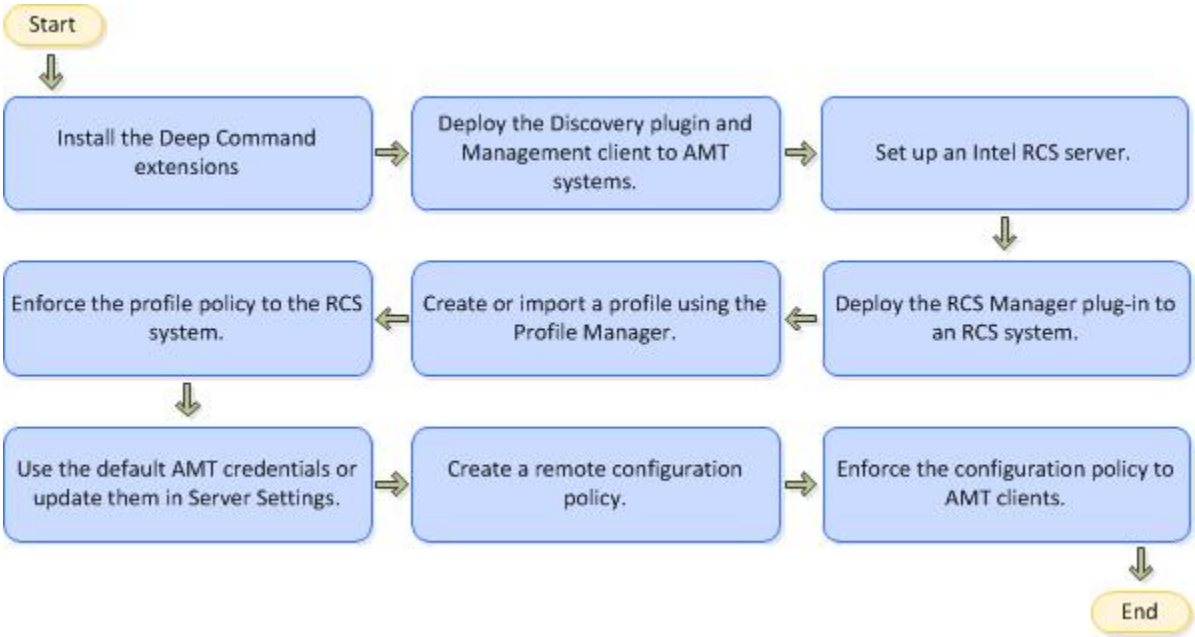
Remote configuration

This method uses Transport Layer Security (TLS) to securely configure Intel® AMT systems.

It requires a configuration server and uses root certificates stored in the Intel® AMT systems. The setup and configuration application identifies itself with a certificate to perform the configuration process.

To implement this method of configuration from McAfee ePO, you need a managed Intel® RCS server with the ePO Deep Command RCS Management plug-in installed on it.

This diagram presents the recommended process for configuring systems using remote configuration.


Start
Install the Deep Command extensions
Deploy the Discovery plugin and Management client to AMT systems.
Set up an Intel RCS server.
Deploy the RCS Manager plug-in to an RCS system.
Create or import a profile using the Profile Manager.
Enforce the profile policy to the RCS system.
Use the default AMT credentials or update them in Server Settings.
Create a remote configuration policy.
Enforce the configuration policy to AMT clients.
End

See also

Perform remote configuration on page 50

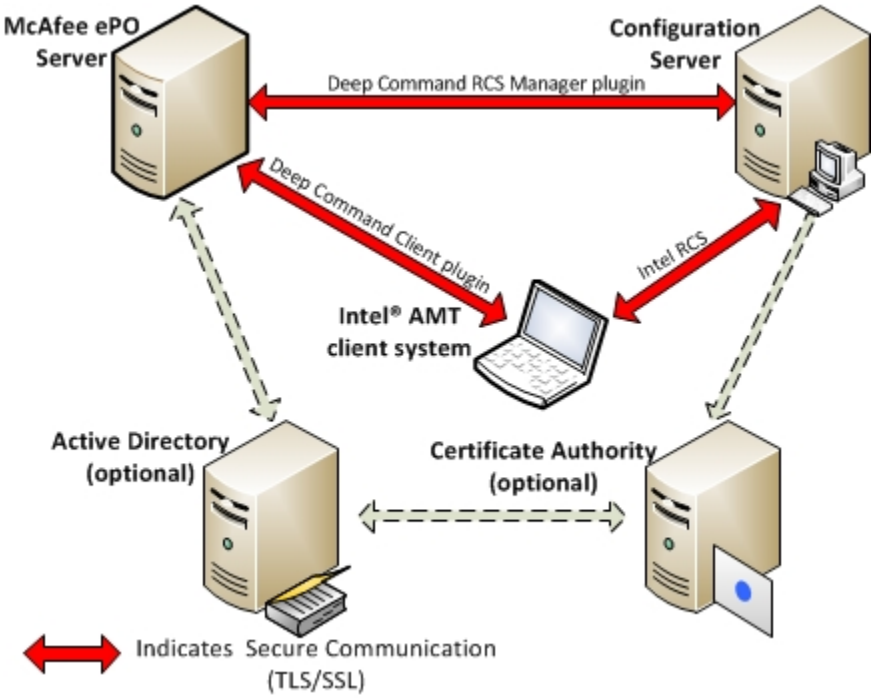
Admin Control mode

Intel® AMT systems enter this mode when they are configured using remote configuration.

Intel® AMT systems in this mode have no limitations to Intel® AMT functionality.

Admin Control mode network architecture

This illustration is an overview of a network configuration where your Intel® AMT systems support Admin Control mode.



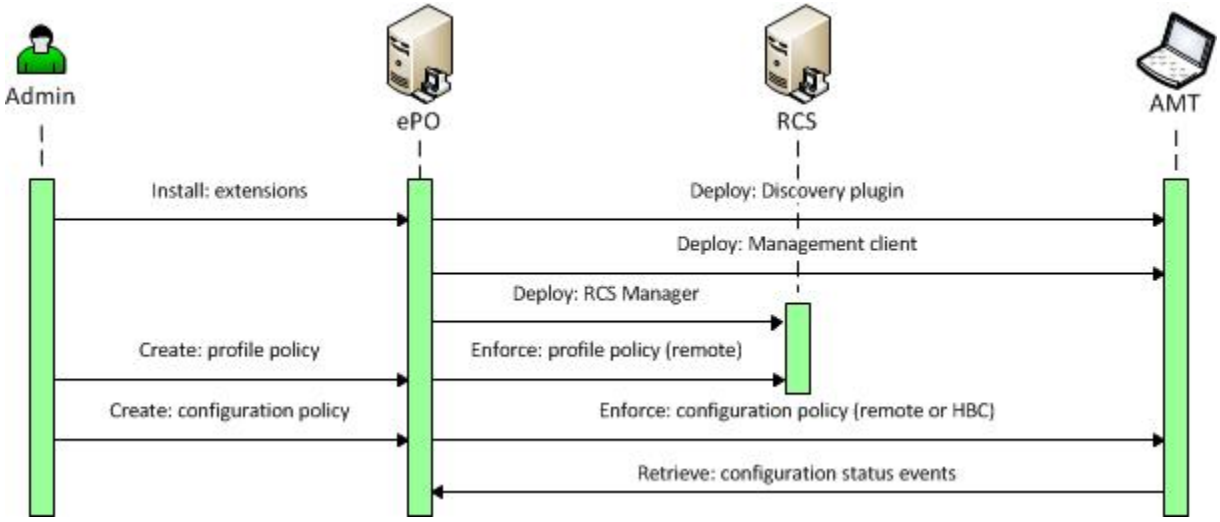
Each of the server components in this illustration performs an essential function in Admin Control mode configuration.

- **McAfee ePO server** — McAfee ePO is the management console where application and enforcement of Intel® AMT policies are configured and distributed. You use the McAfee ePO console to perform these tasks:
  - Modify server settings such as selecting or importing required certificates, providing credentials to authenticate, and enabling communication between McAfee ePO and Intel® AMT systems.
  - Install the ePO Deep Command RCS Manager plug-in, then deploy it to the Intel® RCS system.
  - Create and enforce the configuration policy by selecting the remote configuration options.
- **Configuration server** — Intel® RCS server is used to configure an Intel® AMT system. It automates the process of populating Intel® AMT systems with user names, passwords, and network parameters that enable the system to be administered remotely from ePO Deep Command. Using the RCS Manager plug-in, McAfee ePO can enforce the Intel® AMT configuration policies to the configuration server.
- **Active Directory server** — You can use digest user credentials to authenticate your communication, or Kerberos authentication using an Active Directory (AD) server.
- **Certificate authority server** — McAfee recommends that you use McAfee ePO Deep Command Root CA to simplify the configuration process. However, you can also use an external certificate authority server such as Microsoft CA or a custom root CA. These servers issue certificates to the correct trusted devices within the network. You can use Transport Layer Security (TLS) communication by incorporating certificates issued by a CA.

How RCS Manager plug-in works

The RCS Manager plug-in helps you manage the configuration of your Intel® AMT firmware, through McAfee ePO.

This diagram illustrates the actions involved in configuration through the RCS Manager plug-in.



The RCS Manager retrieves configuration profiles from the Intel® RCS servers, and reports back to McAfee ePO. The server uses these profiles to configure Intel® AMT systems and lists them under the ePO Deep Command configuration policies.

You can create configuration profiles in the Intel® RCS console, then check in the RCS Manager. You then push it to the Intel® RCS server to retrieve the server and profile-related information.

The information is listed in the configuration policy that can be configured based on the selected Intel® RCS server and configuration profile. Customized policies are then pushed to the Intel® AMT system through the McAfee Agent. The ePO Deep Command client initiates the configuration. Once the process is complete, the status for success or failure is sent to McAfee ePO.

Remote configuration authentication

For remote configuration, select a user authentication method, deploy a configuration certificate, and select a server authentication certificate.

User authentication

To configure your systems, your network infrastructure must include a supported authentication method.

Depending on your network requirements, you can use one or both of these supported authentication methods:

- **Digest authentication** — Performed over the Internet using secure keys to authenticate users. For more information, see the Internet Engineering Task Force document RFC 2617.
- **Kerberos authentication** — Performed over an open network as a trusted third-party authentication service. Use of this protocol requires Active Directory integration. For more information, see the Internet Engineering Task Force document RFC 4120.

Certificates for TLS

You can use the Transport Layer Security (TLS) protocol to secure and authenticate communications across your network.

Intel® AMT uses the Public Key Infrastructure (PKI) method of TLS, which provides secure communication using an asymmetric public and private cryptographic key pair. The key pair is retrieved and shared through a trusted authority, known as *Certification Authority (CA)*. The CA supplies digital certificates that can identify an individual or an organization. By default, McAfee ePO Deep Command Root CA issues this certificate. You can also use Microsoft CA.

Remote configuration certificate

For Intel® AMT configuration, you can deploy a vendor-supplied certificate in your network.

To use Public Key Infrastructure (PKI), the Intel® AMT system must have a pre-programmed root certificate hash. When using a vendor-supplied certificate for the configuration, you must:

- Use a supported vendor. The list of supported vendors is based on the root certificate hashes present in the Intel® AMT firmware and its versions. For the list of supported vendors, see http://communities.intel.com/docs/DOC-2225.
- Generate a Certificate Signing Request (CSR) and purchase the appropriate SSL certificate from the vendor. For purchasing the correct SSL certificate, see http://communities.intel.com/docs/DOC-1277.
- Install the vendor certificate on the system where Intel® SCS Remote Configuration Service (RCS) is running. For more information on installing the vendor certificate, see *Installing a Vendor Certificate* in the *Intel® Setup and Configuration Service (Intel® SCS) User Guide*.

Server authentication certificate

A server authentication certificate is required for each Intel® AMT device for TLS.

When the Intel® AMT system is configured to use TLS, the configuration server automatically requests a certificate from the root certificate. You can configure ePO Deep Command to use one of these:

- **McAfee ePO Deep Command Root CA** — When the ePO Deep Command Management Framework component is installed, it also installs a McAfee ePO Deep Command Root CA. This Root CA signs the TLS certificates of the Intel® AMT system. Intel® RCS generates these certificates during the configuration process. The TLS certificate of an Intel® AMT system is used for managing the system.
- **Microsoft CA** — You can set up a Microsoft CA server in a Windows server system. This system acts as a self-signed CA in your network, which can issue certificates for use with public key security programs.
- **Custom CA** — You can use a certificate from a custom root CA. Export the certificate from the root CA with keys, then import it to ePO Deep Command.

Configuration states

ePO Deep Command adds a system property to determine the configuration status of Intel® AMT systems.

- **Pre-configuration** — By default, the Intel® AMT features on Intel® vPro™ systems are disabled because the systems are unconfigured. ePO Deep Command cannot manage such systems remotely. All unconfigured clients are categorized under this state.
- **In-configuration** — While a host-based or remote configuration is in-progress, the Intel® AMT systems are moved from pre-configuration to in-configuration.

  When configuration fails, check whether the system state is still in the in-configuration state. A system in this state might be at risk. We recommend that you resolve the configuration issue, then configure it again.

- **Post-configuration** — When the configuration process is complete, ePO Deep Command can manage the Intel® AMT systems. Such systems are considered in post-configuration.

4 Configuring Intel AMT systems

You can configure an Intel® AMT system using host-based configuration or remote configuration.

- Host-based configuration places the Intel® AMT system in Client Control mode by default. It is the simplest configuration method. McAfee recommends this configuration method. This mode limits some of Intel® AMT functionality.
- Remote configuration places the Intel® AMT system in Admin Control mode by default. In this mode, there are no limitations to Intel® AMT functionality. Use this method when host-based configuration is not sufficient for your business needs such as when your Intel® AMT systems are managed remotely.

Contents

- *Synchronize with Windows Active Directory*
- *Set Intel AMT configuration preferences*
- *Perform host-based configuration*
- *Perform remote configuration*
- *Test your connection to an Intel AMT system*
- *Unconfigure Intel AMT systems through McAfee ePO*

Synchronize with Windows Active Directory

ePO Deep Command acquires users through the Windows Active Directory (AD). You must have a registered LDAP server to use Kerberos authentication.

Tasks

- *Register Windows Active Directory server* on page 43
  It is necessary to register Windows Active Directory with McAfee ePO to use Kerberos authentication.
- *Schedule LDAP synchronization* on page 44
  Create a task to synchronize McAfee ePO with the Active Directory.

Register Windows Active Directory server

It is necessary to register Windows Active Directory with McAfee ePO to use Kerberos authentication.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Configuration** | **Registered Servers**, then click **New Server** to open the Registered Server Builder wizard.
2. On the **Description** page, select **LDAP Server**, specify a unique name and any details, then click **Next**.

3 On the **Details** page, complete these options.

   a Select **Active Directory** from **LDAP server type**, then type the DNS-style domain name or IP address of the system where Windows Active Directory is present.

   When using a DNS-style domain name, make sure that McAfee ePO is configured with the appropriate DNS setting and can resolve the DNS-style domain name of Active Directory.

   b (Optional) Select **Use Global Catalog**, **Chase referrals**, and **Use SSL**, as needed.

   c Type the user name in the format: `domain\user name`.

   d Type the password, then retype it to confirm.

   e Click **Test Connection** to verify that the connection to the server works, then click **Save**.

Schedule LDAP synchronization

Create a task to synchronize McAfee ePO with the Active Directory.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Automation** | **Server Tasks** to open the **Server Tasks** page.

2 Click **Actions** | **New Task** to open the Server Task Builder wizard.

3 On the **Description** page, name the task, add a description about the task, select **Enabled** under **Schedule** status, then click **Next**.

4 From the **Actions** drop-down list, select **LdapSync: Sync across users from LDAP**, select an Active Directory server, then click **Next** to open the **Schedule** page.

5 Schedule the task, then click **Next** to display the **Summary** page.

6 Review the task details, then click **Save**.

   You can also run this task immediately by clicking **Run** next to the task on the **Server Tasks** page.

Set Intel AMT configuration preferences

Set up your environment to perform a host-based or remote configuration.

Configuration profiles provide settings that are required to configure the Intel® AMT systems. Import a profile that you created in Intel® RCS console or by using ACUWizard.exe, or create a profile using the **Configuration Profile** policy. The profile setting modified in McAfee ePO is pushed to the respective profile in Intel® RCS through policy enforcement. For profile creation using Intel® RCS instructions, see *Create a configuration profile in Intel RCS*.

Also, use the default ePO_AMTAdmin user account or update your Intel AMT credentials as per your environment. You can view the auto-generated password on **Server Settings**.

Tasks

- *Import a configuration profile template* on page 45
  Import a configuration profile that you created in the Intel® RCS console or by using ACUWizard.exe.
- *Create a configuration profile* on page 45
  Create a **Configuration Profile** policy for the configuration settings, then enforce it to the Intel® RCS server.
- *Set Intel AMT credentials* on page 48
  A password for Intel® AMT configuration and actions is generated automatically for the default digest user account ePO_AMTAdmin. Use the default credentials or modify them as needed.

Import a configuration profile template

Import a configuration profile that you created in the Intel® RCS console or by using ACUWizard.exe.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Profile Templates**, then click **Edit**.

3 From **Import and Manage Templates**, click **Import**, complete these options in the **Import AMT Template** screen, then click **OK**:

- **Location** — Browse to the template and select it.
- **Name** — Type a name.
- **Password** — Type the password, if encrypted.
- **Confirm Password** — Retype the password to confirm.

The template is listed in the **Imported AMT Templates**.

Create a configuration profile

Create a **Configuration Profile** policy for the configuration settings, then enforce it to the Intel® RCS server.

Before you begin

- To customize a host-based configuration profile, create it in the Intel® RCS console or by using ACUWizard.exe, export the Intel® RCS profile, then import it in McAfee ePO.
- To perform Intel® AMT actions over wireless, create a profile with Wi-Fi settings. See *Create a configuration profile using Intel RCS* for instructions.

Don't enforce the default policies directly to your Intel® AMT systems. They don't contain the required data such as passwords. Also, when you export a configuration profile, passwords and users information is not exported due to security reasons.

Task

Create policies based on the default policies such as **McAfee Default** or **My Default**. The default policies provide templates where you can add the data required to configure your Intel® AMT systems. For option definitions, click **?** in the interface.

1 In the McAfee ePO console, navigate to **Policy Catalog**, select **ePO Deep Command Profile Manager 2.1.0** as the product and **Configuration Profile** as the category, then click **New Policy**.

2 Select **McAfee Default**, type a name for the configuration policy and any notes, then click **OK**.

3 In the **General** tab,

a Type a description for the profile.

b Select a profile template:

- **Default** — Select a default template: **Remote configuration with TLS** or **Host base configuration with TLS**.
- **User** — Select a custom template that you imported. A message appears that states the type of selected profile: remote configuration or host-based configuration.

  To import a new custom template, click **Import**, then

  1 Browse to select a template exported from Intel® RCS console.

  2 Type a name for the template.

  3 Type the password to decrypt the template.

  You can only import a password encrypted profile.

  4 Retype the password to confirm, then click **OK**.

  (Optional) To remove an added template, select it, then click **Delete**.

c Type the Intel® MEBX password, then retype it to confirm.

Select **Show Password** to see the password as you type. Password confirmation is not required with this option.

This step can be used only for a remote configuration template.

d Select **Use generated random password** to use a randomly generated digest password or select **set password**, type a digest password, then retype it to confirm.

Select **Show Password** to see the password as you type. Password confirmation is not required with this option.

The password must match the Intel® AMT credentials entered in **Server Settings**.

e (Optional) Select **Integrate with Active Directory**, then browse to select the Active Directory Organization Units.

f In **AMT User accounts and rights**, perform one of these steps:

- For Digest account, click **New Digest User**, type user name, type password, retype password (or select **Show Password**), then select the required access right for the use:
  - **Administrator** — Provides PT Administration rights, which allows the user to access all Intel® AMT features. A PT Administrator manages security control data such as Access Control Lists, Kerberos parameters, Transport Layer Security, Configuration parameters, power-saving options, and power packages. Also this user has access to all realms.

    If a PT Administrator wants to run configurator to perform host-based configuration, the **Access Type** must be selected as **Local** or **Both**.

  - **Help Desk** — Provides these access rights:
    - **Hardware Asset** — To retrieve information about the hardware inventory of the Intel® AMT system.
    - **Storage** — To configure, and write to and read from non-volatile user storage.
    - **General Info** — To retrieve general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters.
    - **Endpoint Access Control** — To retrieve settings associated with NAC/NAP posture.
    - **Event Log Reader** — To allow definition of a user with permissions only to read the Intel® AMT system log.
    - **User Access Control** — To group ACL management commands into a separate realm to enable users to manage their own passwords without requiring administrator rights.
  - **Remote Power Control** — Provides these access rights:
    - **Redirection** — To enable and disable the redirection capability and retrieves the redirection log.
    - **Remote Control** — To enable powering up a system or shutting it down remotely. Used with the Redirection capability to boot remotely.
    - **General Info** — To retrieve general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters.
  - (Optional) To modify a saved digest account, select it, then click **Edit**.
- For Kerberos account,
  1. Select **New Kerberos User** or **New Kerberos Group**, as needed, select the required user or group, then click **OK**.
  2. Select the user or group, then select the required access right for the user or group (**AMT Administrator**, **AMT Help Desk**, **AMT Remote Power Control**).

4 (Optional) In the **Advanced** tab, complete these Remote configuration options:

- **Remote management** — Select whether to enable the web interface for Intel® AMT management.
- **Intel Fast Call for Help** — Select when a user can initiate a call for help:
  - **OS initiated** — from the operating system.
  - **BIOS initiated** — from the BIOS.

- **IP address** — Select the source for the IP address settings:
  - **DHCP** — from the DHCP server.
  - **Static** — the same IP address as the host.
- **FQDN** — Select the source for the host name suffix:
  - **Primary DNS** — from the "Primary DNS Suffix" of the host operating system.
  - **Active directory name** — from the Active Directory domain where the host operating system is a member.

These options can be used only for a remote configuration template.

5 Save the policy, then list the profile in the Intel® AMT configuration policy page.

Host-based configuration profile	Remote configuration profile
No further action required	1 From **System Tree**, select the Intel® RCS server, click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command Profile Manager 2.1.0** as the product, select **Configuration Profile** as the category, select the policy, select **Break Inheritance**, then save the policy assignment. 2 Enforce the policy using one of these methods: • Wait for the next agent-server communication or send an agent wake-up call. • From the Intel® RCS server, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.

The profile created in McAfee ePO appears in the Intel® AMT configuration policies and is prefixed with **ePO_**.

See also

Create a configuration profile using Intel RCS on page 145
Create a configuration profile that uses Microsoft CA certificates on page 154
Modify ePO Deep Command settings on page 26

Set Intel AMT credentials

A password for Intel® AMT configuration and actions is generated automatically for the default digest user account ePO_AMTAdmin. Use the default credentials or modify them as needed.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit**.

3 In **Credentials for Intel® AMT Configuration**, do one of these:

- **Use the default ePO_Admin account** — Select **Show password** to view the default password.
- **Update credentials** — Select **Change credentials**, then type the digest user name and password to be used for Intel® AMT configuration.

4 In **Credentials for Intel® AMT actions**, do one of these:

- **Use the default ePO_Admin account** — Select **Use above credentials**, then select **Show password** to view the default password.
- **Update credentials** — Select **Change credentials**, deselect **Use above credentials**, then type the user name and password to be used for Intel® AMT actions. (Use `domain\user name` format for Active Directory accounts)

5 Click **Save**.

Perform host-based configuration

Create and enforce a host-based configuration policy which uses the host-based configuration profile.

Before you begin

- Intel® AMT system must support host-based configuration. Navigate to its system properties page, from the **Products** tab select **McAfee ePO Deep Command Client**, then check the value for **Host Based Configuration**.
- Local Manageability Service driver must be present on the Intel® AMT system. Value for **Local Manageability Service Present** in the **Deep Command** tab on the **System Details** page for the client system, must be **Yes**.
- If an Intel® AMT system is already configured and you want to migrate it from Admin Control mode to Client Control mode, unconfigure the client first.

Task

1 In the McAfee ePO console, navigate to **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.

2 In the **New Policy** dialog box, perform these steps:

a Select **McAfee Default**, type a name for the configuration policy and any notes, then click **OK**.

b Select **Allow ePO to enforce these settings**, select **Host based configure to enable Client Control Mode**, then select a host-based profile. If none of the host-based profiles is created in McAfee ePO, the default host-based profile is listed as **Default_HBC_Profile**.

This configuration method doesn't need a configuration server.

c Save the policy.

3 In the **System Tree**, assign the policy to the required systems or group.

- To assign the policy to selected systems, select the systems, click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Configuration Policies** as the category, select the modified configuration policy, select **Break Inheritance**, then save the policy assignment.
- To assign the policy to a system group or to the entire **My Organization** group, select the group, select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Configuration Policies**, select the modified configuration policy under **Assigned policy**, then save the policy assignment.

4 Enforce the policy using one of these methods:

- Wait for the next agent-server communication or send an agent wake-up call.
- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
- Click **Actions** | **AMT Actions** | **Enforce AMT Firmware Configuration Policy**.

Perform remote configuration

Install and configure the RCS Manager plug-in to manage the Intel® AMT firmware configuration from McAfee ePO.

Before you begin

Make sure that the Intel® AMT systems meet the requirements and prerequisites. See *Requirements* and *Prerequisites for remote configuration*.

The RCS Manager plug-in communicates with the Intel® RCS servers for configuration or unconfiguration.

Most of these tasks involve steps that are performed in a non-McAfee environment. This guide covers brief information on settings required for a remote configuration. However, see the *Intel® Setup and Configuration Service (Intel® SCS) User Guide* for detailed information on these steps and for any alternative steps.

Tasks

- *Enable McAfee ePO Deep Command certificates support in Intel RCS* on page 51
  Enable support for third-party certificates in Intel® RCS to recognize McAfee ePO Deep Command Root CA signed certificates.
- *Install the Profile Manager extension* on page 51
  The Profile Manager extension is required to manage the Intel® AMT configuration through McAfee ePO.
- *Check in the RCS Manager package* on page 51
  Check in the RCS Manager package to deploy it to the managed Intel® RCS servers.
- *Deploy the RCS Manager plug-in* on page 52
  Deploy the RCS Manager plug-in to the Intel® RCS server.
- *Configure Intel AMT systems using remote configuration policy* on page 53
  Create and enforce a remote configuration policy and select the Intel® RCS server and configuration profile to be used.

See also

Requirements on page 18
Prerequisites for remote configuration on page 50

Prerequisites for remote configuration

Prepare the Intel® AMT system environment to configure the systems using remote configuration.

- Install and configure Intel® RCS 8.2 or later. Obtain the latest Intel® RCS version and required documentation from the Intel website: http://www.intel.com/go/scs.
- Install and configure ePO Deep Command Management Framework.
- Enable the designated ports in firewall.
- Assign IP addressing in the Dynamic Host Configuration Protocol (DHCP).
- Intel® RCS domain name and FQDN must be resolved from the Intel® AMT systems.
- Intel® AMT systems must not be in wireless mode. To configure wireless clients, use host-based configuration in a wired environment.

- Intel® AMT systems must not be in a virtual private network (VPN) environment. Home domains of McAfee ePO and Intel® AMT systems differ in VPN environment.
- Intel® AMT systems must have an onboard Network Interface Card (NIC). Multiple NICs are not supported.

Enable McAfee ePO Deep Command certificates support in Intel RCS

Enable support for third-party certificates in Intel® RCS to recognize McAfee ePO Deep Command Root CA signed certificates.

Before you begin

Make sure that the Intel® SCS console is closed.

This task is required only when you're using Intel® SCS 8.2 version. For more information on this procedure, see the Intel® SCS 8.2 documentation.

Task

1. In the Intel® SCS server, browse to the installed directory. For example, `C:\Program Files\Intel\SCS8.2\Console\`.
2. Open the `SCSConsole.exe.config` file in a text/xml editor, locate the setting named `SupportCAMediation`, then set its value to `True`.

The Intel® RCS recognizes certificates from third-party CA including the McAfee ePO Deep Command Root CA.

Install the Profile Manager extension

The Profile Manager extension is required to manage the Intel® AMT configuration through McAfee ePO.

Perform this task if you didn't check in this extension with other ePO Deep Command extensions from **Software Manager**.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.
2. On the **Software Manager** page under **Product Categories**, click **Software Not Checked In** | **Licensed**.
3. Select **McAfee ePO Deep Command 2.1** from the products list, select **McAfee ePO Deep Command Profile Manager Extension**, then click **Check In**.

When checked in successfully, the Profile Manager extension appears under **ePO Deep Command** on the **Extensions** page.

Check in the RCS Manager package

Check in the RCS Manager package to deploy it to the managed Intel® RCS servers.

Perform this task if you didn't check in this package with other ePO Deep Command extensions from **Software Manager**.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.
2. On the **Software Manager** page under **Product Categories**, click **Software Not Checked In** | **Licensed**.
3. Select **McAfee ePO Deep Command 2.1** from the products list, select **McAfee ePO Deep Command RCS Manager**, then click **Check In**.

When checked in successfully, the RCS Manager appears under master repository and under **Products and components** on **Product Deployment** page for client tasks.

Deploy the RCS Manager plug-in

Deploy the RCS Manager plug-in to the Intel® RCS server.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, go to **System Tree**, then select the target server hosting Intel® RCS.
2. Click the **Assigned Client Tasks** tab, then click **Actions** | **New Client Task Assignment**.
3. Select **McAfee Agent** under **Product**, and **Product Deployment** under **Task Type**, then click **Create New Task**.
4. Type a name for the task and any notes, then select **Target Platforms**, as needed.
5. In **Products and components**, select **McAfee ePO Deep Command RCS Manager 2.1.0.xxx**, select **Install** as the action, select the language, then click **Save**.
6. Select the task from the list, then click **Next**.
7. Schedule the task to run immediately or as needed, then click **Next**.
8. Review the summary of the task, then click **Save**.

The task is added to the list of client tasks for the selected Intel® RCS server, and is executed at the next agent-server communication.

If the Intel® RCS server is busy, there might be a delay in processing the WMI call. Wait for the next agent-server communication for the RCS Manager information to be updated in the McAfee ePO console.

Configure Intel AMT systems using remote configuration policy

Create and enforce a remote configuration policy and select the Intel® RCS server and configuration profile to be used.

Before you begin

- Make sure that the RCS Manager plug-in properties have been collected. Navigate to the system properties page of the Intel® RCS server, select **McAfee ePO Deep Command RCS Manager Plugin** in the **Products** tab .
- To configure wireless connections, make sure that the clients are present in the wired network during the configuration process. Once the configuration is complete, you can connect to the client using wireless according to the settings provided in the profile used.
- The required WMI and DCOM permissions are applied automatically when you deploy the RCS Manager plug-in. However, if they can't be updated due to any environmental restrictions, the remote configuration might fail. In such scenarios, apply them manually. See *Validate permissions*.

Intel® RCS system uses Windows Management Instrumentation (WMI) to perform remote configuration. There might be a delay in remote configuration if the number of WMI requests on the system exceeds the maximum number of requests that can be processed at a time.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, navigate to **Policy Catalog**, select the **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.
2. In the **New Policy** dialog box,
   a. Select **McAfee Default**, type a name for the configuration policy and any notes, then click **OK**.
   b. Select **Allow ePO to enforce these settings**, then select **Remote configure to enable Admin Control Mode**, select the Intel® RCS server and the profile to be used for the configuration.
   c. Save the policy.
3. In the **System Tree**, assign the policy to the required systems or group.
   - **Systems** — Click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Configuration Policies** as the category, select the modified configuration policy, select **Break Inheritance**, then save the policy assignment.
   - **Group** — Select the group, select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Configuration Policies**, select the modified configuration policy under **Assigned policy**, then save the policy assignment.
4. Enforce the policy using one of these methods:
   - Wait for the next agent-server communication or send an agent wake-up call.
   - From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
   - Click **Actions** | **AMT Actions** | **Enforce AMT Firmware Configuration Policy**.

On successful policy enforcement, the selected Intel® AMT systems are configured for use. To verify, navigate to the **System Properties** page, click the **Deep Command** tab, and make sure that the **Configuration State** is **Post Configuration**.

See also

Create a policy to configure Intel AMT systems on page 94
Enforce Intel AMT configuration policy on page 111

Test your connection to an Intel AMT system

Perform some actions on your Intel® AMT systems to test whether they can be connected.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Systems** | **System Tree**.

2 Select a system that you recently configured, then click **Actions** | **AMT Actions**, then select one of these actions:

- **Power On** — Turns on the Intel® AMT system. See *Turn on your systems* in *Managing your Intel® AMT systems*.
- **Boot/Reboot with Actions** — Provides options to boot the Intel® AMT system. Select **Boot/Reboot from Image (IDE-R)**. See *Boot or reboot using IDE-Redirection* in *Managing your Intel AMT systems*.

See also

Turn on your systems on page 106
Boot or restart using IDE-Redirection on page 109

Unconfigure Intel AMT systems through McAfee ePO

You can unconfigure a managed Intel® AMT system using the configuration policy in the McAfee ePO console.

You can unconfigure a configured system, either completely or partially.

- A complete unconfigure removes the entire configuration (such as the security credentials, and operational network settings) and disables the Intel® AMT features on the system.
- A partial unconfigure retains the configuration data (like the host name, domain name, PKI settings, PSK settings), but disables the Intel® AMT features on the system. The Intel® AMT system can still communicate with the Intel® SCS server.

If a configured Intel® AMT system is outside the home domain and has the Remote Access policy configured, it cannot be unconfigured from McAfee ePO.

Tasks

- *Unconfigure Intel® AMT systems using policy* on page 55
  You can unconfigure your Intel® AMT systems using the Intel® AMT configuration policy.
- *Identify unconfigured systems* on page 55
  Create and execute a query, which retrieves a list of Intel® AMT systems that are unconfigured.
- *Clear the AMT tag* on page 56
  Create a server task based on a query to retrieve the list of unconfigured systems, then set an action to remove the **AMT** tag from them.

Unconfigure Intel® AMT systems using policy

You can unconfigure your Intel® AMT systems using the Intel® AMT configuration policy.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, navigate to **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.

2 In the **New Policy** dialog box, perform these steps:

a Select **McAfee Default**, type a name for the unconfiguration policy and any notes, then click **OK**.

b Select **Allow ePO to enforce these settings**, then perform one of these steps based on configuration mode of systems.

- **Admin Control mode** — Select **Remote configure to enable Admin Control Mode**, select **Unconfigure (if currently configured by ePO)**, and then select the Intel® RCS server and profile used for the configuration.
- **Client Control mode** — Select **Host-based configure to enable Client Control Mode**, select **Unconfigure (if currently configured by ePO)**, and then select the profile used for the configuration. The Intel® AMT systems in this mode do not require an Intel® RCS server. They use the host-based profile to configure or unconfigure the client.

c Select the appropriate unconfigure options.

- **Also remove the pre-shared keys or hash data of self-signed CA certificates configured on the client systems manually.** — To remove the configuration completely (recommended).
- **Force unconfigure even if it is not configured by ePO** — To remove the configuration from a system that was not configured using McAfee ePO.

d Save the policy.

3 In the **System Tree**, assign the policy to the required systems or group.

- **Systems** — Click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Configuration Policies** as the category, select the unconfiguration policy, select **Break Inheritance**, then save the policy assignment.
- **Group** — Select the group, select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Configuration Policies**, select the unconfiguration policy under **Assigned policy**, then save the policy assignment.

4 Enforce the policy using one of these methods:

- Wait for the next agent-server communication or send an agent wake-up call.
- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
- Click **Actions** | **AMT Actions** | **Enforce AMT Firmware Configuration Policy**.

On successful policy enforcement, the selected Intel® AMT system is unconfigured. To verify, navigate to the **System Properties** page, click the **Deep Command** tab, and make sure that the **Configuration State** is **Pre Configuration**.

See also

Create a policy to unconfigure Intel AMT systems on page 94

Identify unconfigured systems

Create and execute a query, which retrieves a list of Intel® AMT systems that are unconfigured.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Reporting** | **Queries & Reports**, then select **ePO Deep Command Reporting** under **Shared Groups**.

2 From the queries list, select **Intel® AMT Configuration State**, click **Action** | **Duplicate**, type a name for the query, then save it.

3 Select the query you created, click **Edit**, then

   a In the **Chart** step, select to display result as **Table**, then click **Next** twice.

   b In the **Filter** step from **Available Properties**, select **Configuration State**, then select **Does not equal** as comparison and **Post Configuration** as its value.

   c Save the query, then execute it.

Clear the AMT tag

Create a server task based on a query to retrieve the list of unconfigured systems, then set an action to remove the **AMT** tag from them.

Before you begin

Create a query to identify unconfigured systems.

Task

1 In the McAfee ePO console, click **Menu** | **Automation** | **Server Tasks**, then click **New Task**.

2 Type a name for the query and a brief description (optional), enable the task, then click **Next**.

3 Select the action as **Run Query**, select the query you created, select **Clear Tag** as the subaction and **AMT** as the tag, then click **Next**.

4 Schedule the task as needed, then click **Next**.

5 Review the task summary, then save it.

6 From the server tasks list, select the task, then click **Run** from the actions.

The **AMT** tag is removed from unconfigured Intel® AMT systems.

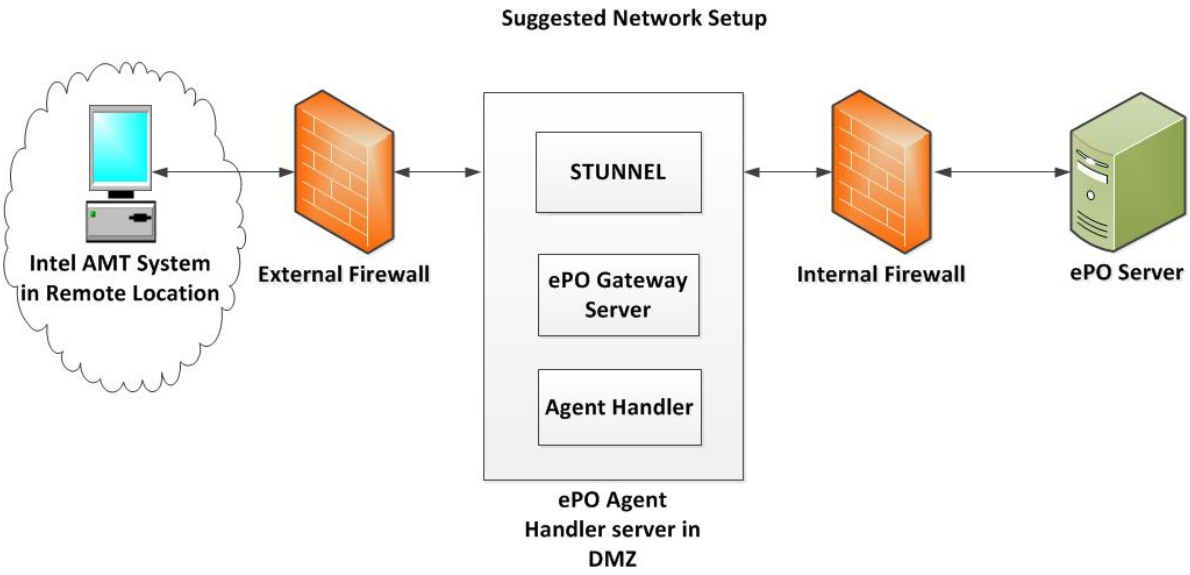
5 Setting up your environment for Remote Access

The McAfee ePO Deep Command Gateway server acts as a proxy responsible for mediating communication between McAfee ePO and remotely managed Intel® AMT systems.

The Remote Access feature allows Intel® AMT systems to initiate a secured connection to the ePO Deep Command Gateway server. The additional required software includes:

- **Gateway server** — One of the ePO Deep Command modules, which allows communication between McAfee ePO and the remote client systems. Install this McAfee software on the DMZ server where the Agent Handler or McAfee ePO is installed. For more information on Agent Handlers and how to configure them, see the McAfee ePO documentation.
- **Stunnel** — An open-source multi-platform program that acts as the SSL tunneling proxy between McAfee ePO and your remote Intel® AMT systems. Download, certify, install, and configure it for the Remote Access feature. For more information on Stunnel and to download it, see http://www.stunnel.org.

Make sure that LAN-based operations are successful and the Intel® AMT systems are accessible from the ePO Deep Command server.



Remote Access depends on these components:

- McAfee ePO
- Intel® AMT systems configured for remote connectivity. (In some environments, these systems are protected with a firewall. If the Intel® AMT system initiates a connection to your server, you can use this connection to administer it.)
- ePO Deep Command Gateway server.
- The ports used in the ePO Deep Command Gateway services are configurable based on your environmental requirements.

Port	Allows
Internet-to-stunnel port	Stunnel to connect to the outside network (Internet). For example, port 2002.
Stunnel-to-gateway (or Intel® AMT listen port)	Stunnel to connect to the Intel® AMT platform. The default port is 11111.
SOCKSv5 proxy-listen port	Gateway server to receive the SOCKSv5 proxy connection requests. The default port is 1080.
HTTP proxy-listen port	Gateway server to receive the HTTP proxy connection requests. Traffic addressed to Intel® AMT platforms through this port is forwarded to the SOCKSv5 port. The default port is 8080.

A Remote Access workflow involves these steps.

- The remote Intel® AMT system or user initiates a connection to the ePO Deep Command Gateway server that acts as a proxy server. The connection is either initiated manually by the user in an operating system level utility, or the pre-operating system level with a key combination. The connection can be scheduled to be initiated automatically according at a predetermined time.
- Once the connection reaches the ePO Deep Command Gateway server, a secure encrypted tunnel back to the Intel® AMT system is established.
- McAfee ePO is notified of the incoming Remote Access request from the Intel® AMT system.
- You can initiate any Intel® AMT system command to the remote Intel® AMT system.

See also

Create a Remote Access policy on page 98

Contents

- *Install the ePO Deep Command Gateway server*
- *Generate certificates for Stunnel*
- *Add DH parameter to the .pem file*
- *Configure Stunnel*
- *Validate certificate*

Install the ePO Deep Command Gateway server

To enable communication with the remotely managed Intel® AMT system, install the ePO Deep Command Gateway server on a server in your corporate DMZ where the Agent Handler is installed.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.
2. On the **Software Manager** page under **Product Categories**, click **Software Not Checked In** | **Licensed**.
3. Select **McAfee ePO Deep Command 2.1** from the products list, select **McAfee ePO Deep Command Gateway Server**, then click **Download**.
4. Extract the package contents to a temporary location on your server in the DMZ where the Agent Handler is installed.
5. Double-click the **SetupAGS.exe** file, then in the **Welcome** page, click **Next**.
6. Select the license type, accept the license agreement, then click **OK**.

   The **Destination Folder** page displays a default folder where the software installation files are copied.
7. Click **Change** to specify a folder, or **Next** to use the default location.
8. Use the default ports for **AMT listen**, **SOCKSv5 Proxy Listen**, and **HTTP Proxy Listen**, or change the ports, as required, then click **Next**.

   If the ports are changed, update the Stunnel configuration file (`stunnel.conf`) with these port numbers. See *Configure Stunnel* for instructions.
9. Click **Install**, then click **Finish**.

Generate certificates for Stunnel

Generate certificates from McAfee ePO Deep Command Root CA to use with Stunnel configuration.

Before you begin

- Install Stunnel on the DMZ server where the Agent Handler or McAfee ePO is installed. See http://www.stunnel.org/ to download and obtain more information on the software.
- Provide published DNS name and IP address in the Agent Handler Settings page. These settings allow an agent to connect to the correct, published, network interface of an Agent Handler. See the McAfee ePO documentation for detailed instructions.

Task

1. In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.
2. In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit**.
3. Click **Generate Certificate Set**, select the Agent Handler, then click **OK**.

   Only Agent Handlers that are enabled and have a Public DNS entry are displayed.
4. Save the `<Agent_Handler_FQDN>.zip` file to your computer, then extract its content.

   The `.zip` contains these files:
   - `CN_McAfee_ePO_Deep_Command_Root.crt` — Public Root Certificate
   - `<Agent_Handler_FQDN>.crt` — Signed certificate
   - `<Agent_Handler_FQDN>.key` — Private key

5 Copy the files to the Stunnel installation directory. For example, `C:\Program Files (x86)\stunnel`.

You can also rename these files:

- `CN_McAfee_ePO_Deep_Command_Root.crt` to `ca.cer`
- `<Agent_Handler_FQDN>.key` to `cira.key`
- `<Agent_Handler_FQDN>.crt` to `cira.pem`

Add DH parameter to the .pem file

The created PEM certificate file needs Diffie-Hellman (DH) values appended to the end. This is done via the OpenSSL tools.

Task

1 In the server where OpenSSL is installed, run the following command in the `\bin` folder under the OpenSSL directory.

```
Openssl dhparam -outform PEM -out dHParam.pem 1024
```

The `dhParam.pem` file is created in the same directory.

2 Open the `dhParam.pem` file in a text editor, then copy its content.

3 On the server where you saved the Stunnel configuration files, browse to the Stunnel installation directory, then locate the `.pem` file created using McAfee ePO. For example, `cira.pem`.

4 Open the `.pem` file in a text editor, add the copied content from `dhParam.pem` file at the end, then save it.

Configure Stunnel

Modify the stunnel.conf file to specify the location for the certificates generated, ports used, and other options.

Task

1 Open the Stunnel configuration file at `C:\Program Files\stunnel\stunnel.conf` and add this content:

```
cert = C:\Program Files (x86)\stunnel\cira.pem
key = C:\Program Files (x86)\stunnel\cira.key
CAfile = C:\Program Files (x86)\stunnel\ca.cer
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
options = NO_SSLv3
options = NO_SSLv2
ciphers = AES128-SHA
verify = 1
debug = 7
output = C:\Program Files (x86)\stunnel\stunnel.log
client = no
[ciraamt]
accept  = 12345
connect = 11111
```

2 In **cert**, **key**, and **CAfile**, replace the file names and location for `cira.pem`, `cira.key`, and `ca.cer` respectively with the actual values.

3 In **ciraamt**, use the default ports or replace them with the ports used.

- **accept** — Port that listens to the incoming Remote Access requests, then forwards it to the port used for the connection. The default port is 81. If you want to use a different port, replace it with the actual port number.
- **connect** — Port that receives the Remote Access requests from the port used for **accept** for establishing the connection. This port must be the same as **AMT Listen Port** configured during the ePO Deep Command Gateway server installation.

Rules must be enabled to allow inbound connections to the Remote Access empty port. In this case, inbound connections must be allowed to port configured for **accept**.

Validate certificate

Verify that the certificate issued to the host name of your ePO Deep Command Gateway server is correct.

Perform these steps from a local system.

Task

1 Using Microsoft Internet Explorer, go to `https://<FQDN of the ePO Deep Command Gateway server>:12345` (or the port you configured in `stunnel.conf` to listen).

2 View the certificate installed on the site.

The certificate must be installed on the ePO Deep Command Gateway server (see its host name) and issued by a CA, which is known to the Intel® AMT system.

6 Enabling Intel AMT wireless manageability

With Intel® AMT over a wireless connection, you can perform Intel® AMT actions on systems within the enterprise or to a properly configured Remote Access scenario.

Make sure that the required wireless settings are configured. Also, consider these guidelines for Intel® AMT management in a wireless environment.

- A wireless connection is established using Wireless network interface (WLAN) or an interface driver (executing on the Intel® AMT system). If you turn off the wireless transmitter or receiver using either a hardware or software switch, Intel® AMT cannot use the wireless interface under any conditions.
- Intel® AMT supports wireless manageability in all System power states (s0-s5). However, the power settings and other parameters must be configured.
- A connection request from the system is authenticated using a wireless profile that contains names, passwords, and other security elements. A user or an administrator defines these profiles using a tool such as Intel® PROSet or the wireless software. However, if the host driver is active and the system is within the enterprise, you can connect to an Intel® AMT system without a wireless profile.
- When there is a problem with the wireless driver while the Intel® AMT system is still on, the system can be connected using wireless network interface.
- Intel® AMT management over wireless operates per the state of the system.
  - If the system is disconnected from the network and not actively using the wireless network interface, Intel® AMT traffic operates similar to a wired environment.
  - If the system is actively using the wireless network interface, Intel® AMT over wireless traffic is intercepted and redirected through Intel® AMT drivers within the operating system.
  - If an operating system transitions from online to offline, Intel® AMT communications gets interrupted momentarily.

Contents

- *Prerequisites for using wireless with ePO Deep Command*
- *Wireless profiles*
- *Wireless profile synchronization*
- *Create a delta configuration profile for wireless*
- *Validate wireless settings*

Prerequisites for using wireless with ePO Deep Command

Consider these guidelines while performing Intel® AMT actions on the wireless clients.

- Intel® AMT over wireless requires the infrastructure to support WPA or WPA2 wireless security.
- For Admin profiles, Temporal Key Integrity Protocol (TKIP) or Counter mode CBC MAC Protocol (CCMP) encryption algorithms must be used. For user profiles, encryption is not mandatory.
- The wireless profile settings must be applied to the Intel® AMT systems. See *Create a configuration profile using RCS*.
- When a wireless client is powered-off, the connection is established using the wireless settings in Management Engine without a need of operating system interface.
- Intel® AMT system must be configured to use DHCP. For Intel® AMT to work with a wireless LAN, it must share IP addresses with the host.
- Desktop platforms must have an onboard wireless adapter.
- The maximum out-of-band speed for the Intel® MEI is 40 Mbps.

Wireless profiles

A wireless profile contains names, passwords, and other security elements to authenticate the system to the wireless Access Point.

These two types of wireless profiles are used for Intel® AMT management:

- **Admin profiles** — Added by an administrator during the configuration profile creation on an Intel® RCS system. These profiles are created using TKIP or CCMP with minimum WPA encryption. They can be viewed from Intel® AMT web interface.
- **User profiles** — Created by the user or defined by a script or installation procedure. These profiles can be created using the WEP encryption or without any encryption. They're not viewable from Intel® AMT web interface.

  When a new wireless network is detected, Intel® PROSet or the Intel® Management and Security Status application (IMSS) displays a message to synchronize the currently active profile with Intel® AMT. The wireless driver transfers the profile and Intel® AMT saves it as a user profile.

  Make sure that your system is not set to block Intel® PROSet pop-up messages.

Wireless profile synchronization

A wireless profile are synchronized between the Intel® Manageability Engine and the operating system on certain events to allow Intel® AMT management.

An Intel® AMT wireless profile is updated when:

- A system is connected to a new wireless network.
- Currently connected profile is pushed to Intel® Manageability Engine.
- Intel® PROSet driver has been reset or updated.
- A wireless password has changed. An admin profile synchronizes automatically during the maintenance task or delta configuration task. A user profile has to be reset manually.

An Intel® AMT wireless profile might not be updated when:

- A profile with similar "SSID" is present on the system.
- The system is configured again with the same profile or a delta configuration has been performed.
- Intel® Local Manageability Service driver is not installed or running.
- A wireless password has changed. For admin profiles, an administrator must run the maintenance or delta configuration task. For user profiles, the user needs to locally reset the Intel® PROSet interface or delete the profile manually from Intel® PROSet.

When you add a user profile on an Intel® AMT system that already has the maximum number of profiles, the oldest profile is deleted to accommodate the new profile.

When you unconfigure a system, all wireless profiles are deleted. When you reconfigure a system, only the admin profiles for the system are deleted.

For more information on wireless profile synchronization, see the *Intel® PROSet/Wireless WiFi Connection Utility User's Guide*.

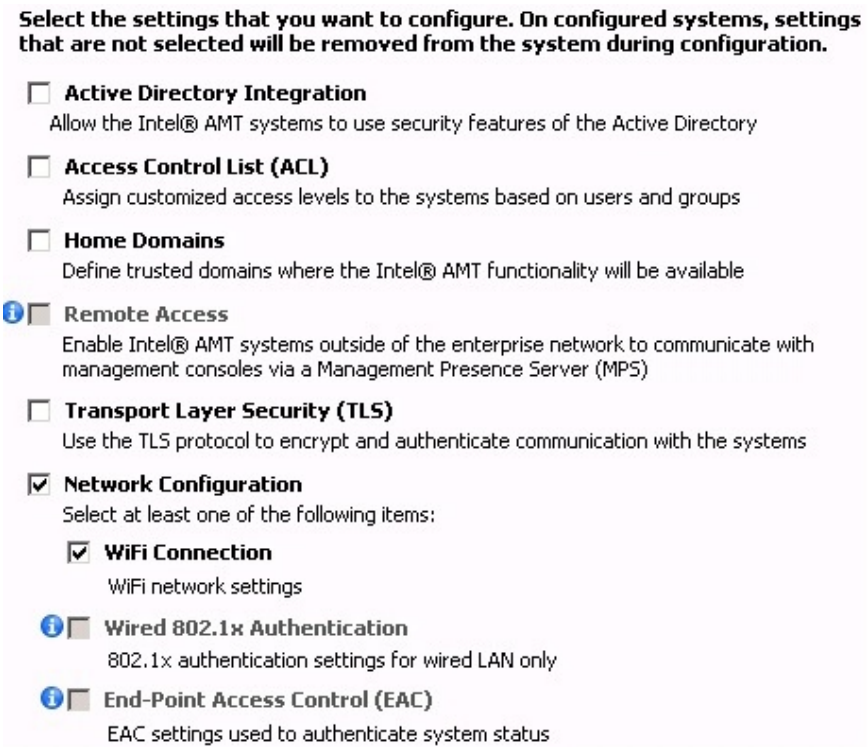
Create a delta configuration profile for wireless

Create delta configuration profiles for the configured systems to add wireless settings without changing any other configuration.

Task

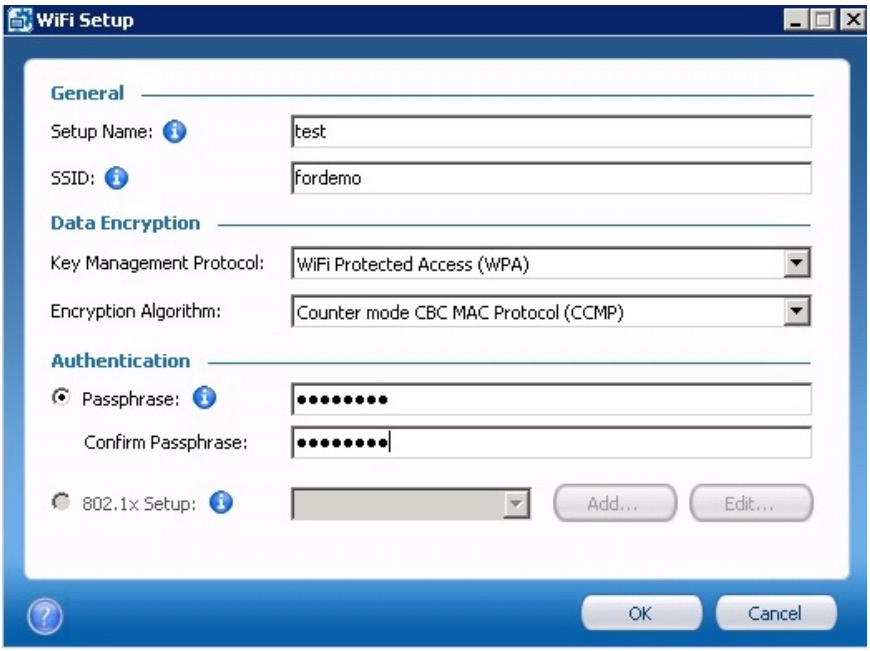
1. From the Intel® SCS Console, click the icon to create a profile, type a unique name, type any description, then click **OK** to open the **Configuration Profile** wizard.
2. On the **Getting Started** page, select **Delta Configuration**, then click **Next**.
3. On the **Profile Scope** page, select **Clear All** and select only **WiFi Connection**, then click **Next**.

4 On the **Optional Settings** page, select **Network Configuration**, select **WiFi Connection**, then click **Next**.


Select the settings that you want to configure. On configured systems, settings that are not selected will be removed from the system during configuration.
Active Directory Integration
Allow the Intel® AMT systems to use security features of the Active Directory
Access Control List (ACL)
Assign customized access levels to the systems based on users and groups
Home Domains
Define trusted domains where the Intel® AMT functionality will be available
Remote Access
Enable Intel® AMT systems outside of the enterprise network to communicate with management consoles via a Management Presence Server (MPS)
Transport Layer Security (TLS)
Use the TLS protocol to encrypt and authenticate communication with the systems
Network Configuration
Select at least one of the following items:
WiFi Connection
WiFi network settings
Wired 802.1x Authentication
802.1x authentication settings for wired LAN only
End-Point Access Control (EAC)
EAC settings used to authenticate system status

5 On the **Network Configuration** page, perform these steps, then click **Next**.

a Select **Allow WiFi connection with the following WiFi setups**, then click **Add** to open the **WiFi Setup** screen.



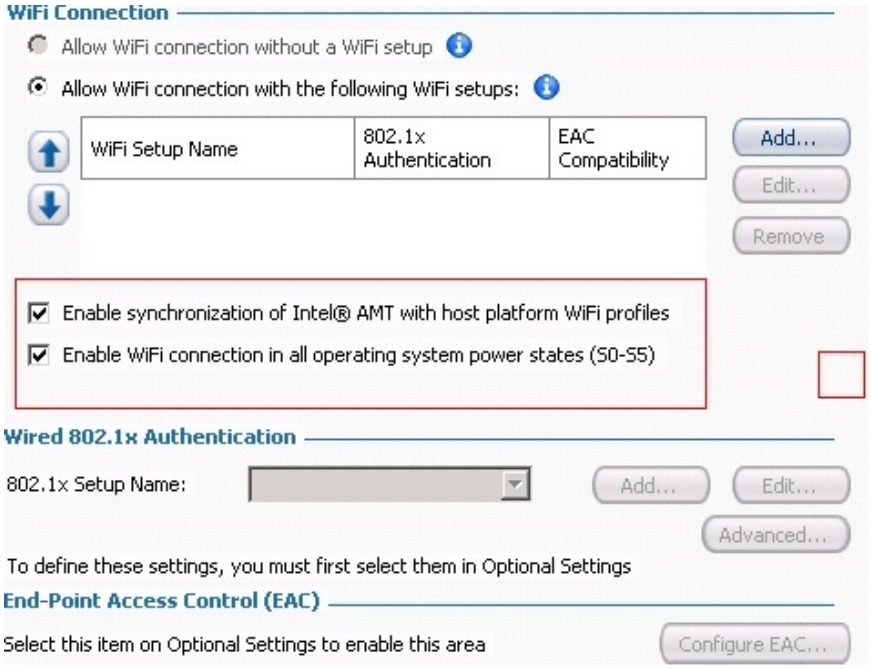
These settings are required to establish connection to wireless Intel® AMT systems. However, the client must have a wired connection during the configuration process.

b Complete these settings, then click **OK**.

- **Setup Name** — Type a name for the Wi-Fi setup (up to 32 characters, and must not contain (/ \ < >: ; * |? ”) characters).
- **SSID** — Type the Service Set Identifier (up to 32 characters) that identifies the specific Wi-Fi network. (If left empty, the device tries to connect to all Wi-Fi networks that use Data Encryption as defined in this Wi-Fi Setup.
- **Key Management Protocol** — Select **WiFi Protected Access (WPA)** or **Robust Security Network (RSN)**, as needed.
- **Encryption Algorithm** — Select **Temporal Key Integrity Protocol (TKIP)** or **Counter mode CBC MAC Protocol (CCMP)**, as needed.
- **Authentication** — Select **Passphrase**, type a password to establish the Wi-Fi connection, then retype it to confirm.

c Select these options:

- **Enable synchronization of Intel AMT with host platform WiFi profiles**
- **Enable WiFi connection in all operating system power states (S0-S5)**


WiFi Connection
Allow WiFi connection without a WiFi setup
Allow WiFi connection with the following WiFi setups:
WiFi Setup Name
802.1x Authentication
EAC Compatibility
Add...
Edit...
Remove
Enable synchronization of Intel® AMT with host platform WiFi profiles
Enable WiFi connection in all operating system power states (S0-S5)
Wired 802.1x Authentication
802.1x Setup Name:
Add...
Edit...
Advanced...
To define these settings, you must first select them in Optional Settings
End-Point Access Control (EAC)
Select this item on Optional Settings to enable this area
Configure EAC...

6 On the **System Settings** page, select **Synchronize Intel® AMT clock with operating system**, as needed, then click **Next**.

7 Click **Finish** to close **Configuration Profile** wizard.

8 Import this profile to McAfee ePO, create a configuration policy to use this profile, then enforce it to the Intel AMT systems. See *Configuring Intel AMT systems*.

Validate wireless settings

Check the Intel® AMT system details in McAfee ePO to validate whether the correct wireless settings have been applied.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, navigate to **System Tree** and open the system details of the wireless client.

2 From the **Deep Command** tab, validate these settings:

- **Wired IPv4 address** — Must be 0.0.0.0.
- **Wireless IPv4 address** — Must be correct.

7 Reporting on your Intel AMT systems

With the ePO Deep Command Discovery and Reporting software, you can quickly determine the status of the Intel® AMT systems in your network.

The predefined queries and dashboards provide you with built-in functionality, since they are added to McAfee ePO when the software is installed. These queries can be configured to display results in charts or tables, which can also be used as dashboard monitors. Query results can be exported to several formats, which can be downloaded or sent as an attachment to an email message.

You can also create custom queries based on the properties collected by the ePO Deep Command Discovery and Reporting plug-in. For details on how to use custom queries, see the McAfee ePO documentation for your version of the software.

Contents

- *Queries and reports*
- *Dashboards and monitors*
- *ePO Deep Command system properties*

Queries and reports

You can create queries on Intel® AMT information stored in the database, or use predefined ePO Deep Command queries.

Predefined reporting queries

When the Discovery and Reporting software is installed on McAfee ePO, these predefined queries are added to the **ePO Deep Command Reporting** group.

Query	Description
AMT-Capable Systems without the Intel® MEI Driver	Displays the number of managed systems that support Intel® AMT but do not have the Intel® MEI driver installed on them.
CILA Supported	Displays a pie-chart of detected client systems supporting Local Access, also known as CILA or Fast Call For Help.
ePO Deep Command Detection Coverage	Displays a pie-chart of the deployment status of the ePO Deep Command plug-in.
IDE Redirect Supported and Enabled	Displays a pie-chart of detected systems that have IDE-Redirection supported and enabled.
Intel® AMT Configuration Mode	Displays a pie-chart of different Intel® AMT configuration modes for all detected systems supporting Intel® AMT. • **Enterprise** — This mode requires a configuration service to configure the systems remotely. • **None** — This configuration status means that no specific mode is selected.

Query	Description
Intel® AMT Configuration State	Displays a pie-chart of different Intel® AMT configuration states for all detected systems supporting Intel® AMT. • **In** (In-configuration) — These systems are in a partially configured state with initial information. • **Post** (Post-configuration) — These systems are in a fully configured state with security settings, certificates, and settings that activate Intel® AMT capabilities. • **Pre** (Pre-configuration) — These systems have factory default settings and don't have any Intel® AMT configuration defined.
Intel® AMT Supported	Displays a pie-chart of managed systems supporting Intel® AMT.
Intel® AMT Version	Displays a column chart of detected Intel® AMT versions.
KVM Supported and Enabled	Displays a pie-chart of detected systems that have Keyboard, Video, and Mouse (KVM) supported and enabled. The KVM might not work on a platform with discrete graphics even if it's supported and enabled. The Intel® AMT KVM operates only with Intel® Integrated Graphics.
Power on remote devices	Displays a pie-chart representing the number of Intel® AMT systems that can be turned on remotely.
Quick reset of pre-boot password on McAfee encrypted devices	Displays a pie-chart representing the number of Intel® AMT systems that can reset their pre-boot password using EEPC to regain their access.
Ready for Host Based Configuration	Displays a pie-chart of the number of Intel® AMT systems that meet and do not meet host-based configuration requirements.
Ready for Remote Configuration	Displays a pie-chart of the number of Intel® AMT systems that meet and do not meet remote configuration requirements.
Remediate or reconfigure remote devices	Displays a pie-chart representing the number of Intel® AMT systems that can be reconfigured remotely.
Secure unlock of pre-boot on McAfee encrypted devices	Displays a pie-chart representing the number of Intel® AMT systems that can automatically unlock their pre-boot password using EEPC for device maintenance.
SOL Supported and Enabled	Displays a pie-chart of detected systems that have Serial-over-LAN (SOL) supported and enabled.
Systems with AMT Tag	Displays a summary table of managed systems that have the AMT tag applied to them.
Troubleshoot Remote Devices (KVM)	Displays a pie-chart representing the number of Intel® AMT systems that can be accessed using McAfee KVM to troubleshoot any issues.
Wake-up devices for security scans and updates	Displays a pie-chart representing the number of Intel® AMT systems that can automatically update their security signatures and patches.
Web UI Enabled Systems	Displays a pie-chart of the number of managed systems that have the Intel® AMT web user interface enabled.

Predefined RCS management queries

When the Profile Manager software is installed on McAfee ePO, these predefined queries are added to the **ePO Deep Command RCS Management** group.

Query	Description
Managed Intel® AMT Systems by RCS Server	Displays a pie chart of Intel® AMT systems categorized by Intel® RCS servers that configured them. The Intel® AMT systems that were configured using host-based configuration are categorized under **Not Available**. From this report, you can click an entry for information on the Intel® AMT systems for the selected category. For the systems configured using remote configuration, the drill-down page also lists their configuration states and Intel® RCS profile used for their configuration.
Managed Intel® RCS Servers	Displays a table of managed Intel® RCS servers. Details include Configuration Profiles, Digest Master Password State, and Network Timeout.

Predefined management queries

When the Management Framework software is installed on McAfee ePO, these predefined queries are added to the **ePO Deep Command Management** group.

Query	Description
ePO Deep Command Policy Settings Report	Displays the ePO Deep Command Policy Settings for managed systems that have the AMT tag applied to them.
Intel® AMT CILA/CIRA Events and KVM Details over Time	Displays a histogram of the CILA/CIRA events over time. From this report, you can click an entry for specific information on events such as event type, configuration state, KVM properties. If caller identification is enabled, you can see events of CILA_User/CIRA_User.
Intel® AMT Configuration Events by Event type	Displays the number of configuration events for all detected Intel® AMT systems. From this report, you can click an entry for information on the Intel® AMT systems for the selected category. For a system configured using remote configuration, the drill-down page also lists the Intel® RCS server name and profile used for its configuration.
Intel® AMT Configuration State and Profile	Displays the number of Intel® AMT systems by their configuration states: **Pre Configuration**, **In Configuration**, **Post Configuration**, and **Not Available**. Systems under **Not Available** category include the Intel® AMT systems that were configured using host-based configuration. From this report, you can click an entry for information on the Intel® AMT systems for the selected category. For the systems configured using remote configuration, the drill-down page also lists the Intel® RCS server name and profile used for their configuration.
Intel® AMT Configuration State by Domain Breakdown	Displays the number of Intel® AMT systems for each configuration state (**Pre Configuration**, **In Configuration**, **Post Configuration**, and **Not Available**) by their domains. Systems under **Not Available** category include the Intel® AMT systems that were configured using host-based configuration.
Local Fast Call For Help Events (CILA)	Displays a summary table of local Fast Call For Help events generated by managed systems supporting Intel® AMT.
Remote Fast Call For Help Events (CIRA)	Displays a summary table of Remote Fast Call For Help events generated by managed systems supporting Intel® AMT.

View default queries

Run the predefined queries to generate reports based on ePO Deep Command components.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Reporting** | **Queries & Reports**.

2 From the **Groups** pane, select **ePO Deep Command Reporting**, **ePO Deep Command Management**, or **ePO Deep Command RCS Management**, as needed.

> In McAfee ePO 4.6, these reports are grouped under **Shared Groups**. In McAfee ePO 5.0, these reports are grouped under **McAfee Groups**.

The queries for the selected group appear.

3 Select a query from the **Queries** list, then click **Run**. In the query result page, click any item in the results to drill down further.

4 Click **Close** when finished.

Custom query filters

You can create custom queries with ePO Deep Command specific filters to retrieve information on your client systems.

> You see these filters only on queries resulting from information about managed systems.

Group	Filter	Filters the results based on...
McAfee ePO Deep Command Client Properties	**Hotfix/Patch Version (McAfee ePO Deep Command Client)**	The patch version of the ePO Deep Command Management Framework software installed on Intel® AMT systems.
	Language (McAfee ePO Deep Command Client)	The localized language of the ePO Deep Command Management Framework software installed Intel® AMT systems. The ePO Deep Command Client is available only in English.
	Product Version (McAfee ePO Deep Command Client)	The version of the ePO Deep Command Management Framework software installed on Intel® AMT systems.
	Service Pack (McAfee ePO Deep Command Client)	The version of the Service Pack installed on Intel® AMT systems.
McAfee ePO Deep Command Detection Plugin Properties	**Product Version (McAfee ePO Deep Command Detection Plugin)**	The version of the ePO Deep Command Discovery and Reporting software installed on Intel® AMT systems.
McAfee ePO Deep Command RCS Manager Plugin Properties	**Language (McAfee ePO Deep Command RCS Manager Plugin)**	The localized language of the ePO Deep Command RCS Manager plug-in installed on managed Intel® RCS servers. The ePO Deep Command RCS Manager plug-in is available only in English.
	Product Version (McAfee ePO Deep Command RCS Manager plugin)	The version of the ePO Deep Command RCS Manager software on managed Intel® RCS servers.
Intel® AMT	**Alarm Enabled**	Whether the ePO Deep Command AMT policy has been scheduled to turn on Intel® AMT systems.

Group	Filter	Filters the results based on...
	BIOS Release Date	The release date of the BIOS running on Intel® AMT systems.
	BIOS Version	The version number of the BIOS running on Intel® AMT systems.
	CILA	Whether the Client-Initiated Local Access (CILA), also known as Fast Call for Help feature, is supported and enabled on Intel® AMT systems.
	CILA Agent Handler	The FQDN of the Agent Handler assigned by the ePO Deep Command Local Access policy to handle CILA requests generated by Intel® AMT systems.
	CILA Enabled	Whether ePO Deep Command Local Access policy has enabled and enforced CILA on Intel® AMT systems.
	CIRA Agent Handler	The FQDN of the DMZ Agent Handler assigned by ePO Deep Command Remote Access policy to handle Client-Initiated Remote Access (CIRA) requests generated by Intel® AMT systems.
	CIRA Enabled	Whether the ePO Deep Command Remote Access policy has enabled and enforced CIRA on Intel® AMT systems.
	Configuration Mode	The Configuration Mode used to configure Intel® AMT systems.
	Configuration Mode (TLS)	The TLS configuration mode of Intel® AMT systems.
	Configuration State	The configuration state of Intel® AMT systems.
	DHCP Enabled	Whether DHCP is enabled on Intel® AMT systems.
	Endpoint Access Control Enabled	Whether Intel Endpoint Access Control is enabled to check for Intel® AMT Network Policy Compliance on client systems.
	Firmware Update Enabled	Whether the Firmware Update feature is enabled in the BIOS of Intel® AMT systems.
	Firmware Version	The version number of the firmware running on Intel® AMT systems.
	Hardware Crypto Enabled	Whether the Intel® AMT hardware crypto engine feature is enabled on Intel® AMT systems. If disabled, the Transport Layer Security doesn't work.
	IDE Redirection (IDE-R)	Whether the IDE-R feature is supported and enabled on Intel® AMT systems.
	Intel® AMT DNS Name	The full Domain Name System name stored in the Intel® AMT firmware on Intel® AMT systems.
	Intel® AMT Fully Configured	Whether the Intel® AMT hardware is fully configured.
	Intel® AMT Supported	Whether the systems are equipped with Intel® AMT hardware.
	Intel® AMT Version	The version number of the Intel® AMT hardware present on systems.
	Intel® AMT Anti-Theft Supported	Whether the systems support Intel® Anti-Theft technology.
	Intel® MEI Enabled	Whether the MEI driver is present and turned on.
	Intel® MEI Version	The version number of the MEI driver running on Intel® AMT systems.
	Intel® vPro™ System	Whether the target systems are Intel® vPro™ systems.

Group	Filter	Filters the results based on...
	KVM	Whether the KVM (Keyboard, Video and Mouse switch) feature is supported on Intel® AMT systems.
	Last Error Message	The error description for the error that occurred if the last AMT action failed.
	Last IDE-R Session Start/End Time	The time when the last IDE-R session was initiated or stopped.
	Last EDI-R Session Status	Whether the status of the last IDE-R Session was active.
	Last Power On Success	Whether the last attempt to power systems on through alarm clock AMT action was successful.
	Last Power On Time	The time this system was powered on last through alarm clock AMT action.
	Last SOL Session Start/End Time	The time when the last SOL session was initiated or stopped.
	Last SOL Session Status	Whether the status of the last SOL Session was active.
	Local Manageability Service Present	Whether the Intel® Local Manageability Service driver is present.
	Manageability Level	The manageability level of Intel® AMT systems.
	Mobile System (Laptop)	Whether Intel® AMT systems are laptops.
	Network Interface Enabled	Whether the network interface is enabled on Intel® AMT systems.
	Policy Enforced	Whether the ePO Deep Command AMT policy is enforced on client systems.
	Policy Enforcement Time	The last enforcement time for the ePO Deep Command AMT policy on client systems.
	Remote Configuration Enabled	Whether the Intel® AMT systems can be configured remotely.
	Remote Configuration Server	The FQDN of the Intel® RCS server used for configuring Intel® AMT systems.
	Remote Configuration Server IP Address	The IP address of the Intel® RCS server used for configuring Intel® AMT systems.
	Serial-over-LAN (SOL)	Whether the SOL feature is supported and enabled on Intel® AMT systems.
	System Manufacturer	Filters the results based on manufacturer of the client systems.
	System Model	The model number of the client systems.
	System Serial Number	The serial number of the client systems.
	TLS	Whether Intel® AMT systems are in Configured State with TLS enabled (required to configure and manage Intel® AMT systems through ePO Deep Command).
	User Consent Mode Required	Whether user consent is required for applying Intel® AMT actions on these systems.
	UUID	The ID of the Intel® AMT systems' hardware.
	Web UI Enabled	Whether the Intel® AMT web interface was enabled on the client systems during the configuration.
	Wired IPv4 Address	The IPv4 address of the Intel® AMT systems' physical network connection.

Group	Filter	Filters the results based on...
	Wired Link Status	Whether Intel® AMT systems' physical network connection is functioning.
	Wired MAC Address	The MAC address of the Intel® AMT systems' physical network connection.
	Wireless Ipv4 Address	The IPv4 address of the Intel® AMT systems' wireless network connection.
	Wireless Link Status	Whether Intel® AMT systems' wireless network connection is functioning.
	Wireless MAC Address	The MAC address of the Intel® AMT systems' wireless network connection.
Intel® AMT Management	**Configuration Profile**	The configuration profile used in configuring the Intel® AMT systems.
	Control Mode	The current configuration mode of the Intel® AMT systems: **Client Control Mode**, **Admin Control Mode**, or **Unconfigured**.
	Host-Based Configuration	Whether the host-based configuration is supported on the system: **Supported** or **Not Supported**.
	Is Embedded HBC Enabled	Whether the host-based configuration is enabled on the system.
	RCS Server	The Intel® RCS server used in configuring the Intel® AMT systems.
Intel® RCS Management	**Digest Master Password State**	Whether the Intel® RCS server profile is configured to use a Digest Master Password.
	Network Timeout (seconds)	The time set for which the Intel® RCS tries to establish a connection.
	RCS Profiles	Filters the configuration profiles configured on the Intel® RCS server.

Dashboards and monitors

Dashboards, which are comprised of monitors, help you keep track of your managed Intel® AMT systems.

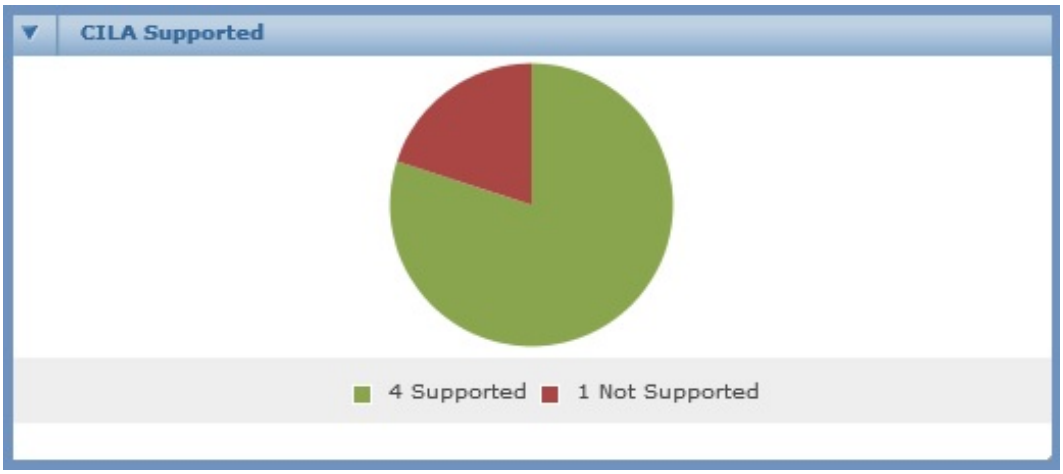
In McAfee ePO 4.6, these dashboards are grouped under **Public Dashboards**. In McAfee ePO 5.0, these dashboards are grouped under **McAfee Dashboards**.

Discovery and Reporting Summary dashboard

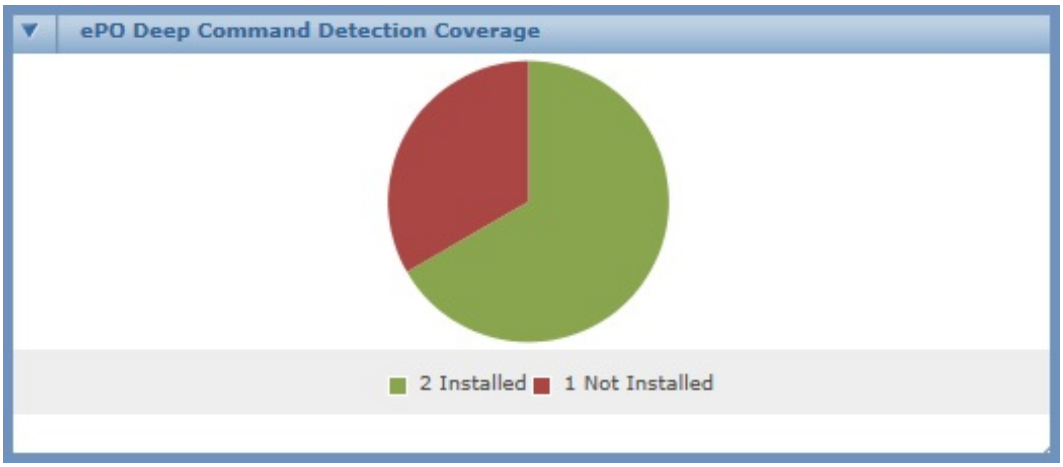
The **Discovery and Reporting Summary** dashboard displays a collection of monitors based on the default ePO Deep Command Reporting query results.

These are the default monitors that appear under the **Discovery & Reporting Summary** dashboard:

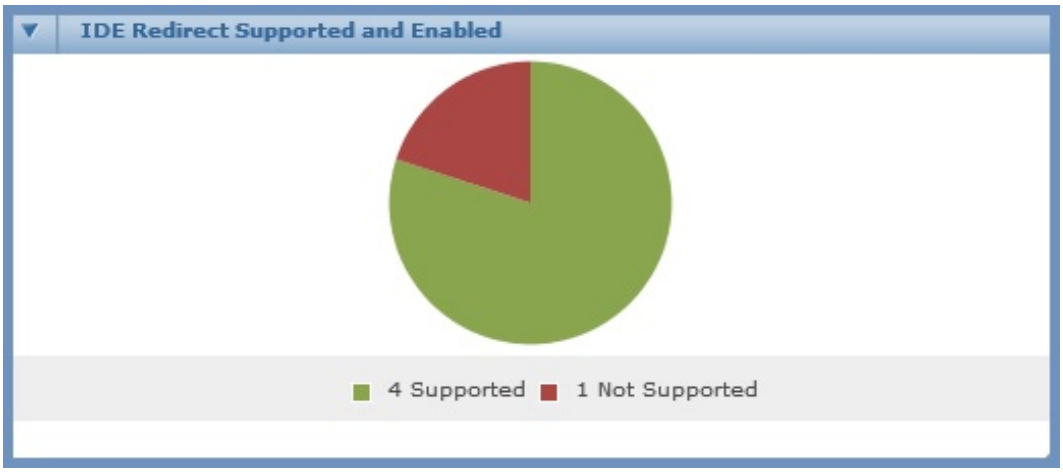
- **CILA Supported** — Determines the number of managed systems that support Local Access connections out of the total number of managed systems. The administrator can then determine the number of managed systems to enforce Local Access Policy that enables Local Access support. This information allows the managed systems to send Local Access requests to McAfee ePO.



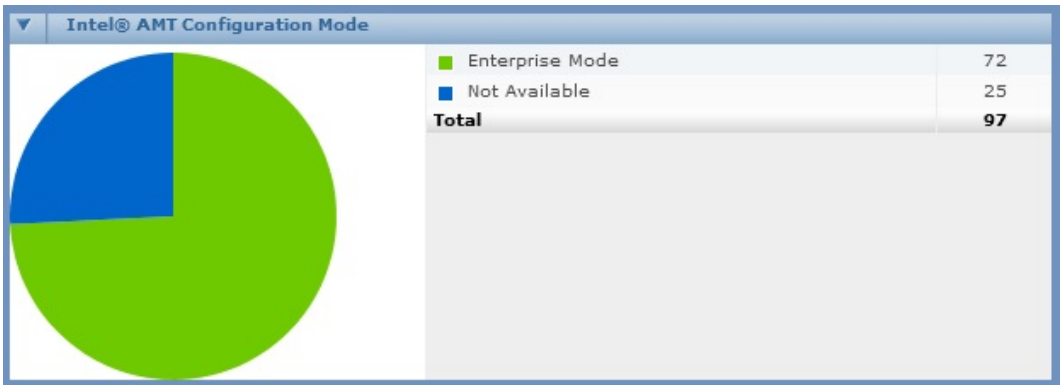
- **ePO Deep Command Detection Coverage** — Determines the number of managed systems where the ePO Deep Command Discovery and Reporting plug-in has been installed, out of the total number of managed systems. This monitor is useful to determine the coverage of the software.



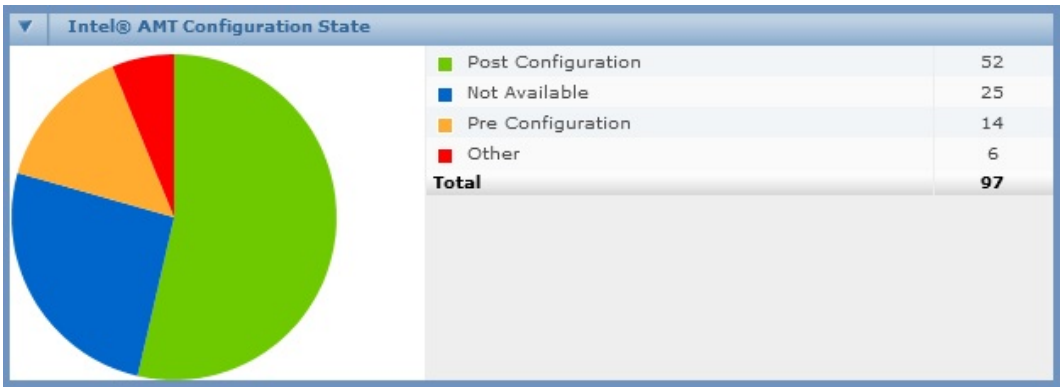
- **IDE Redirect Supported and Enabled** — Determines the number of managed systems that support IDE-Redirection and are configured to remotely managed them using IDE-Redirection connections.



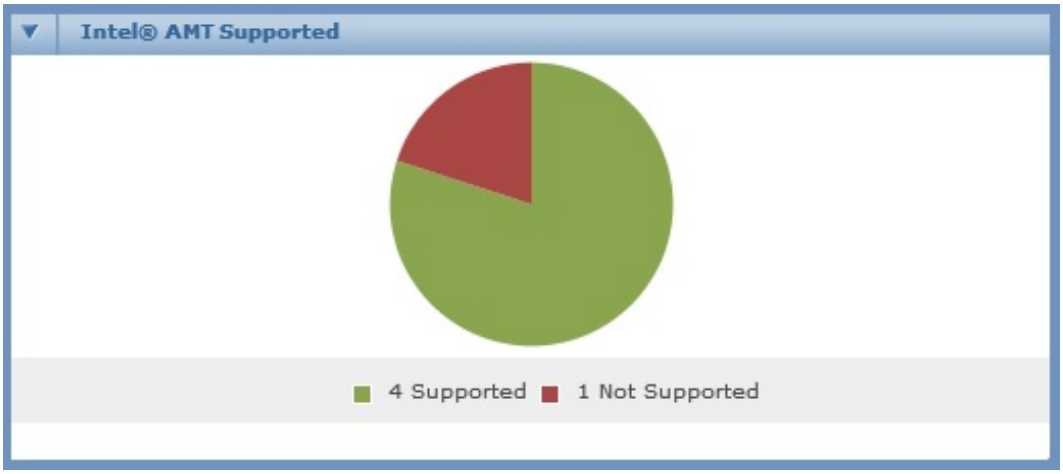
- **Intel® AMT Configuration Mode** — Determines the different configuration modes that are present in the total number of managed systems. Because ePO Deep Command currently supports the Enterprise mode only, the administrator must reconfigure managed systems that are not in Enterprise mode.



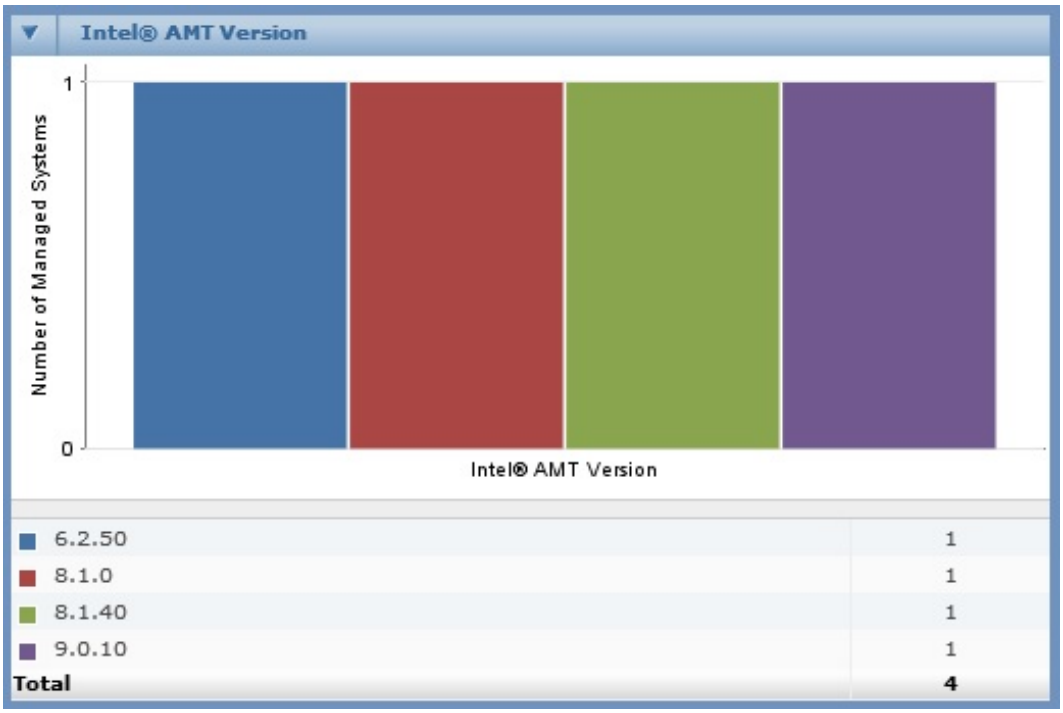
- **Intel® AMT Configuration State** — Determines the different Intel® AMT configuration states present in the total number of managed systems. The Intel® AMT actions can be used on any managed system that is in the Post Configuration state.



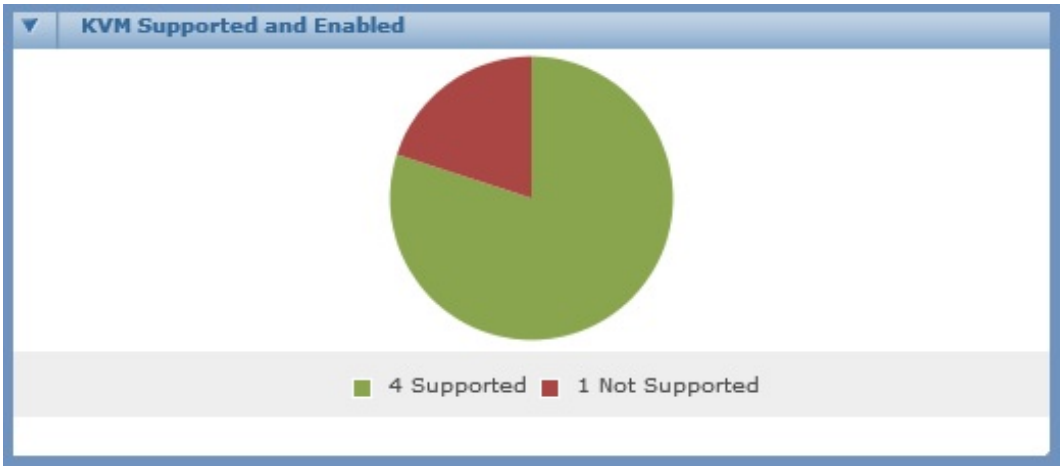
- **Intel® AMT Supported** — Determines the number of managed systems that are Intel® AMT-equipped. However, Intel® AMT actions might not be possible on all these systems; they depend on the Intel® AMT version and the configuration state.



- **Intel® AMT Version** — Displays the different versions of Intel® AMT hardware present on the managed systems. Because ePO Deep Command supports specific versions of Intel® AMT, this monitor determines how many systems can be used for Intel® AMT actions.

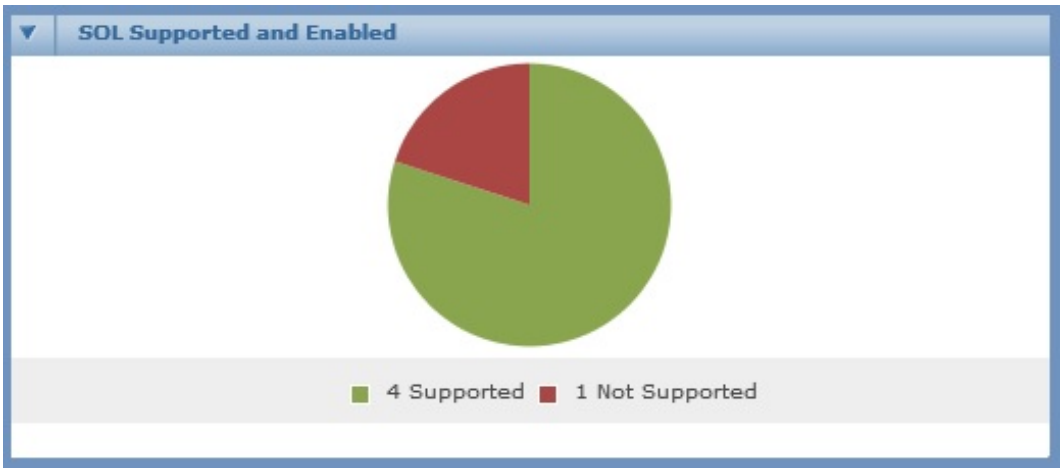


- **KVM Supported and Enabled** — Displays the number of managed systems that support KVM connections out of the total number of managed system. This monitor determines the number of systems that can be managed remotely using KVM.

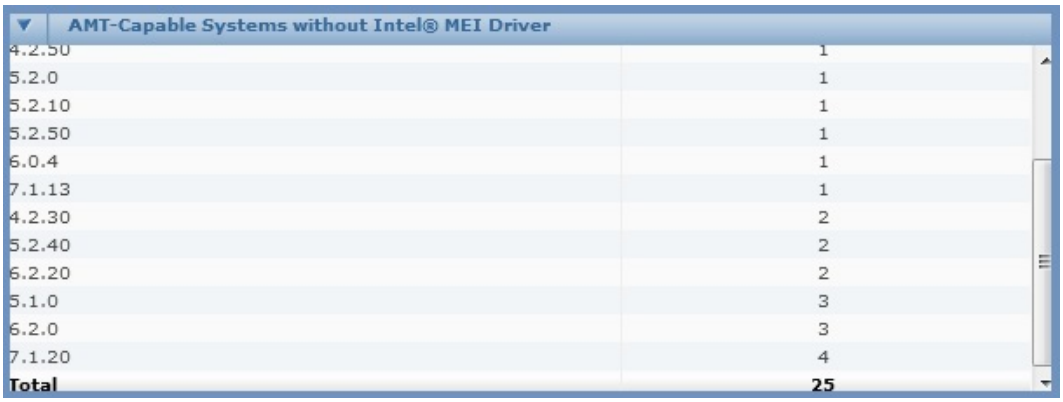


The KVM might not work on a platform with discrete graphics even if it's supported and enabled. The Intel® AMT KVM only operates with Intel® Integrated Graphics.

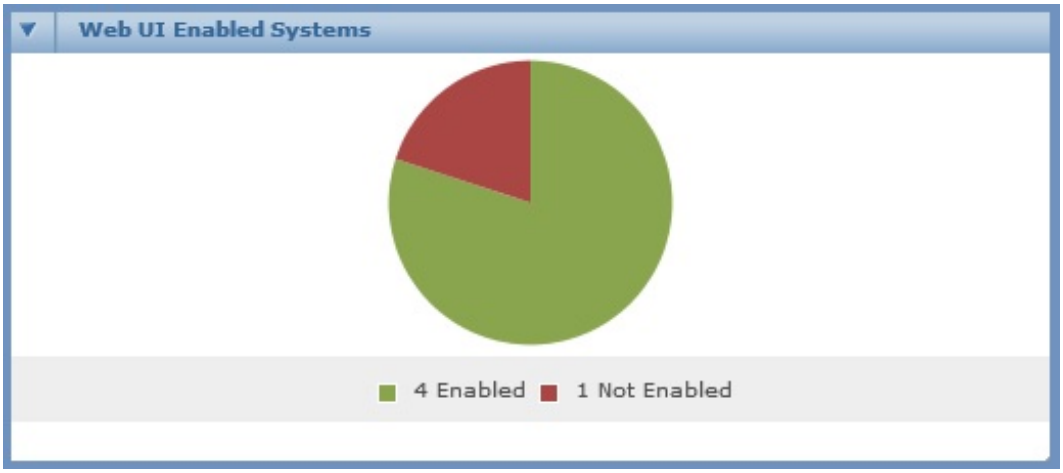
- **SOL Supported and Enabled** — Displays the number of managed systems that support SOL connections out of the total number of managed systems. This monitor determines the number of systems that can be managed remotely using SOL.



- **AMT-Capable Systems without Intel® MEI Driver** — Determines the systems that require installation of the MEI driver out of the total number of managed systems. The systems without Intel® MEI driver cannot collect specific Intel® AMT and BIOS properties.



- **Web UI Enabled Systems** — Determines the number of managed systems that support web browsers. The administrator can open the browser and connect to the managed system using its fully qualified domain name (FQDN) to 16993 port, and log on to it.



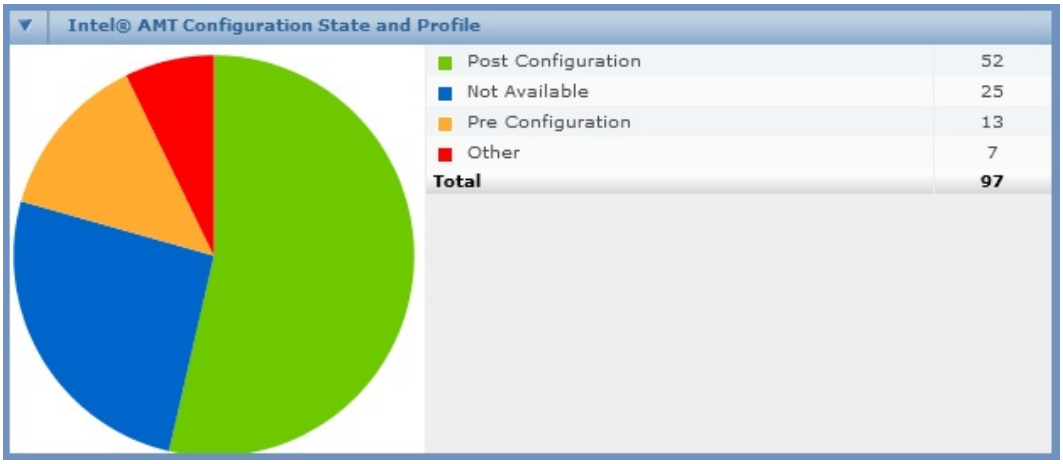
For more information on Intel® AMT and BIOS properties of each managed system, click the monitor, select the system, then click the **Deep Command** tab.

Management Summary dashboard

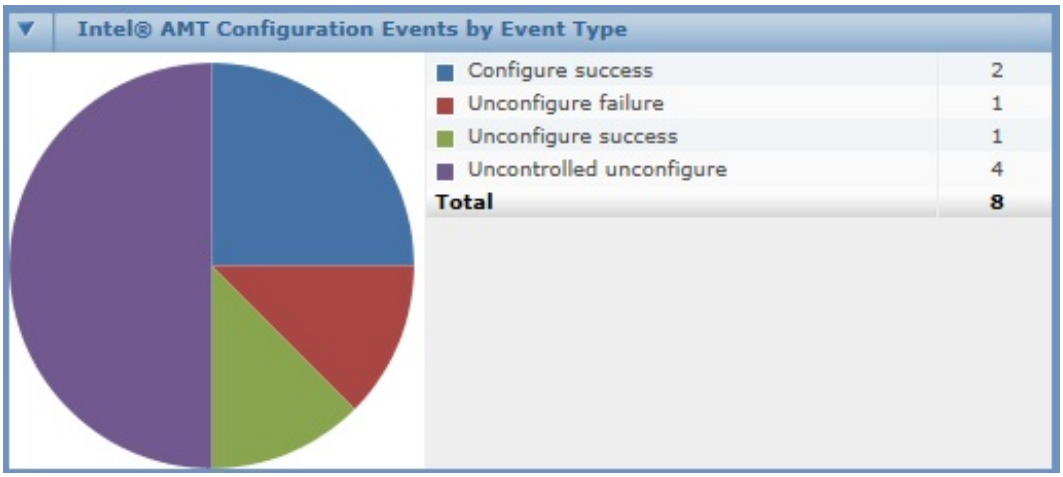
The **Management Summary** dashboard displays a collection of monitors based on the results of the default ePO Deep Command Framework software queries.

These are the default monitors that appear under the **Management Summary** dashboard:

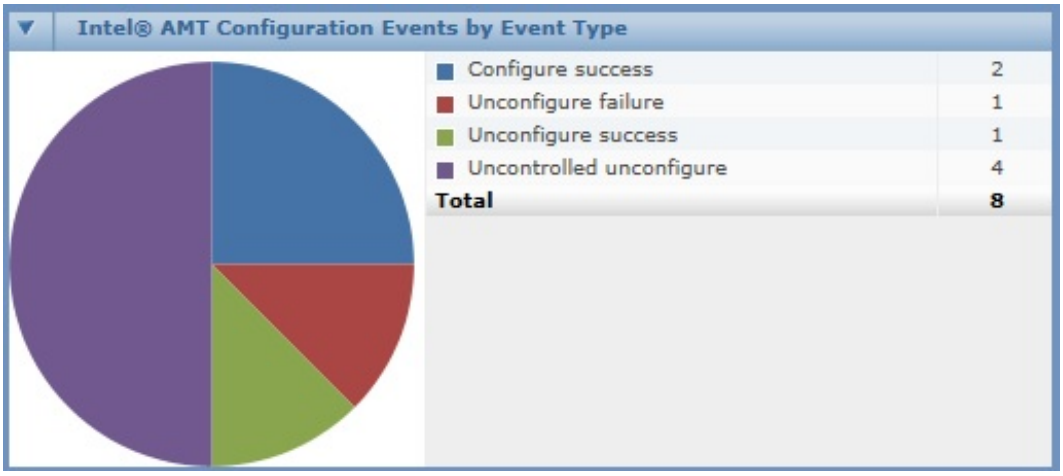
- **Intel® AMT Configuration State and Profile** — Displays a pie chart representing the number of Intel® AMT systems by their configuration states: **Pre Configuration**, **In Configuration**, **Post Configuration**, and **Not Available**. Systems under **Not Available** include the Intel® AMT systems that were configured using host-based configuration.



- **Intel® AMT Configuration State by Domain Breakdown** — Displays a bubble chart representing the number of Intel® AMT systems for each configuration state (**Pre Configuration**, **In Configuration**, **Post Configuration**, and **Not Available**) by their domains. Systems under **Not Available** include the Intel® AMT systems that were configured using host-based configuration.



- **Intel® AMT Configuration Events by Event type** — Displays a pie chart representing the number of configuration events for all detected Intel® AMT systems.



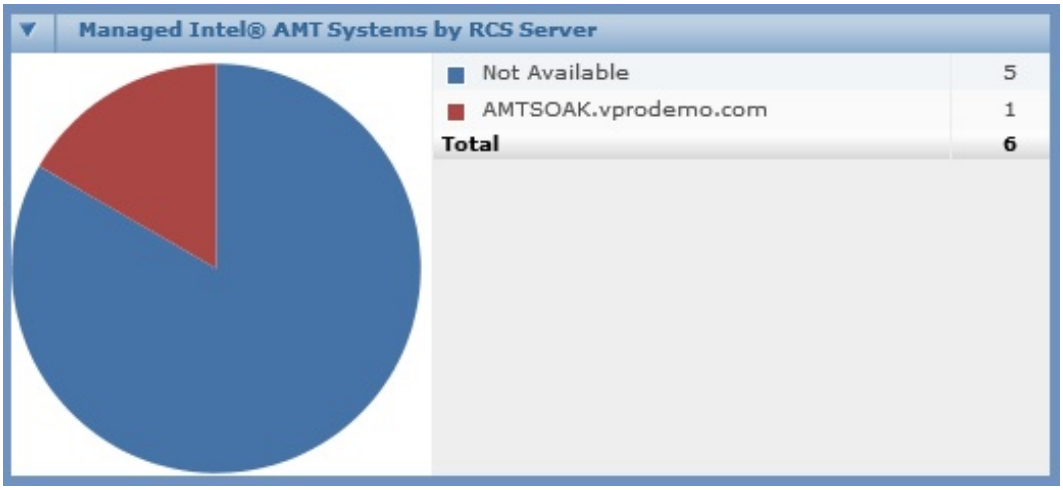
From any of these reports, you can click an entry for information on the Intel® AMT systems for the selected category. For the systems configured using remote configuration, the drill-down page also lists the Intel® RCS server name and profile used for their configuration.

RCS Management Summary dashboard

The **RCS Management Summary** dashboard displays the number of Intel® AMT systems by their respective Intel® RCS servers.

This monitor is the default monitor that appears under the **RCS Management Summary** dashboard:

- **Managed Intel® AMT systems by RCS server** — Displays a pie chart of Intel® AMT systems categorized by Intel® RCS servers that configured them. The Intel® AMT systems that were configured using host-based configuration are categorized under **Not Available**. From this report, you can click an entry for information on the Intel® AMT systems for the selected category. For the systems configured using remote configuration, the drill-down page also lists their configuration states and Intel® RCS profile used for their configuration.

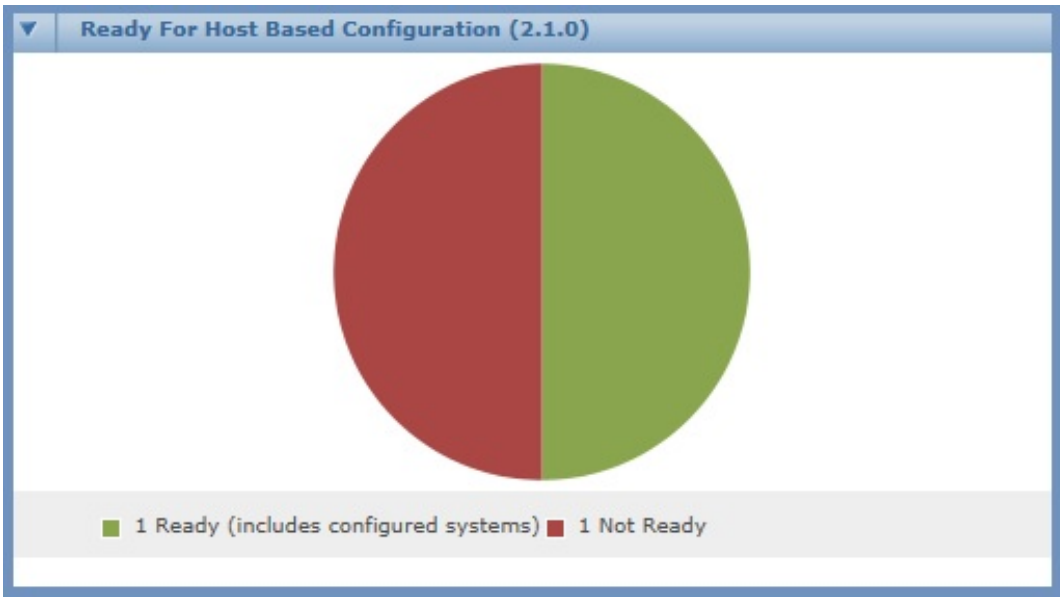


Readiness Summary dashboard

The **Readiness Summary** dashboard includes a monitor that display the count of Intel® AMT systems that meet and do not meet the requirements for host-based configuration.

These are the default monitors that appear under the **Readiness Summary** dashboard:

- **Ready for Host Based Configuration** — Displays a pie-chart representing the number of Intel® AMT systems that meet and that do not meet the host-based configuration requirements. The number of systems that are ready for host-based configuration include the number of systems that are already configured.

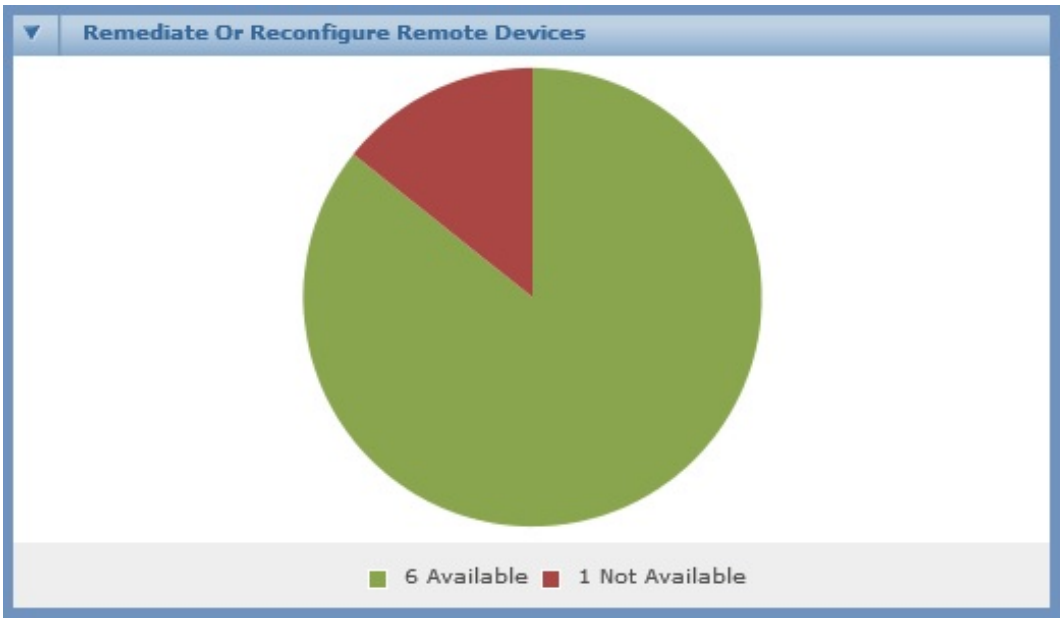


Benefits Summary dashboard

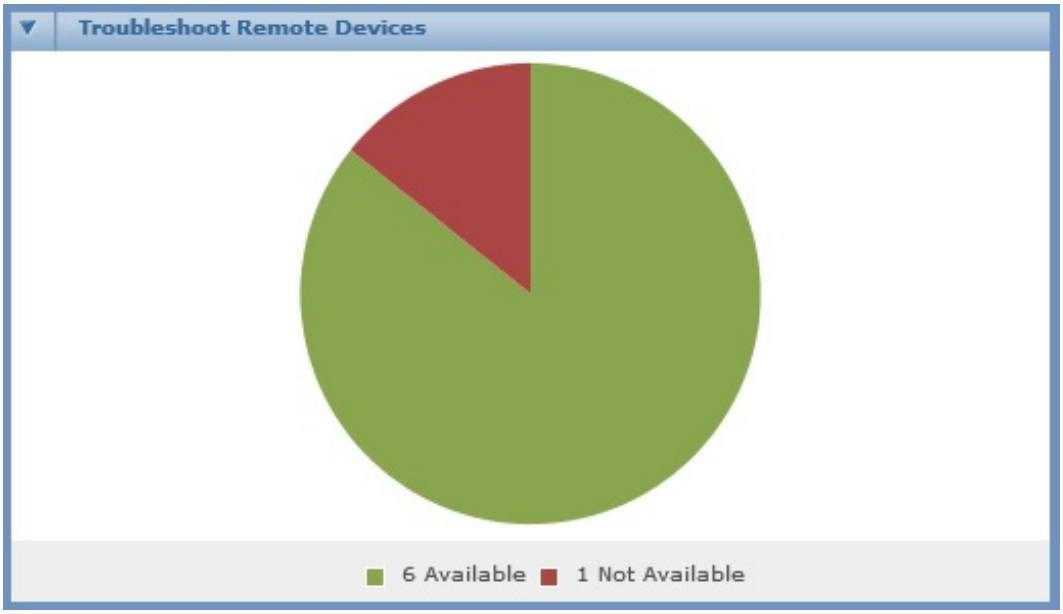
The **Benefits Summary** dashboard displays monitors that display the count of systems by Intel® AMT features.

These are the default monitors that appear under the **Readiness Summary** dashboard:

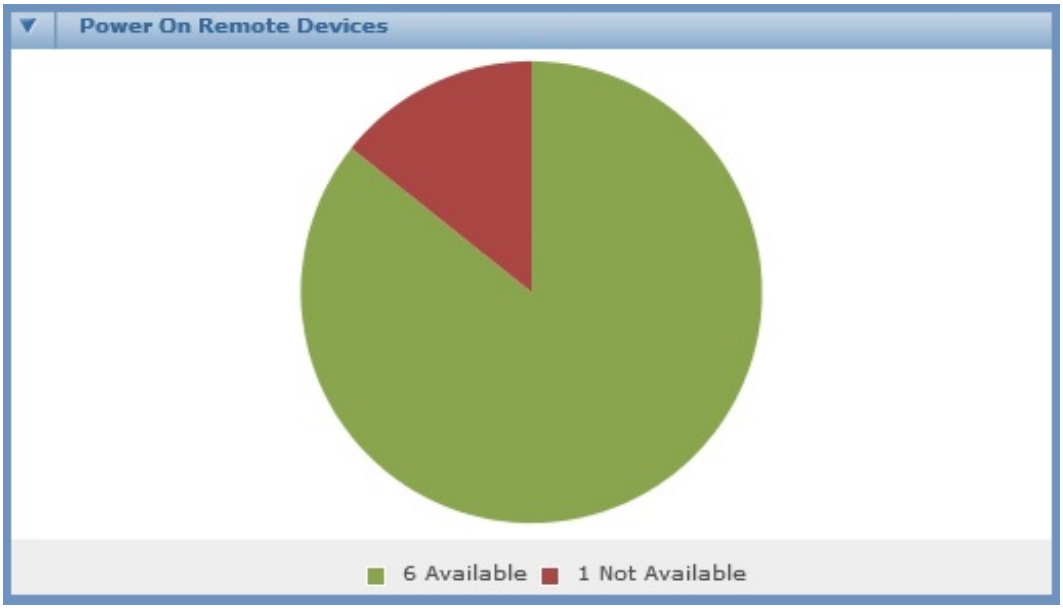
- **Remediate or reconfigure remote devices** — Displays a pie-chart representing the number of Intel® AMT systems that can be reconfigured remotely. Systems in this category meet these conditions:
  - Intel® AMT 4.0 or later — installed
  - IDE-Redirection — supported and enabled



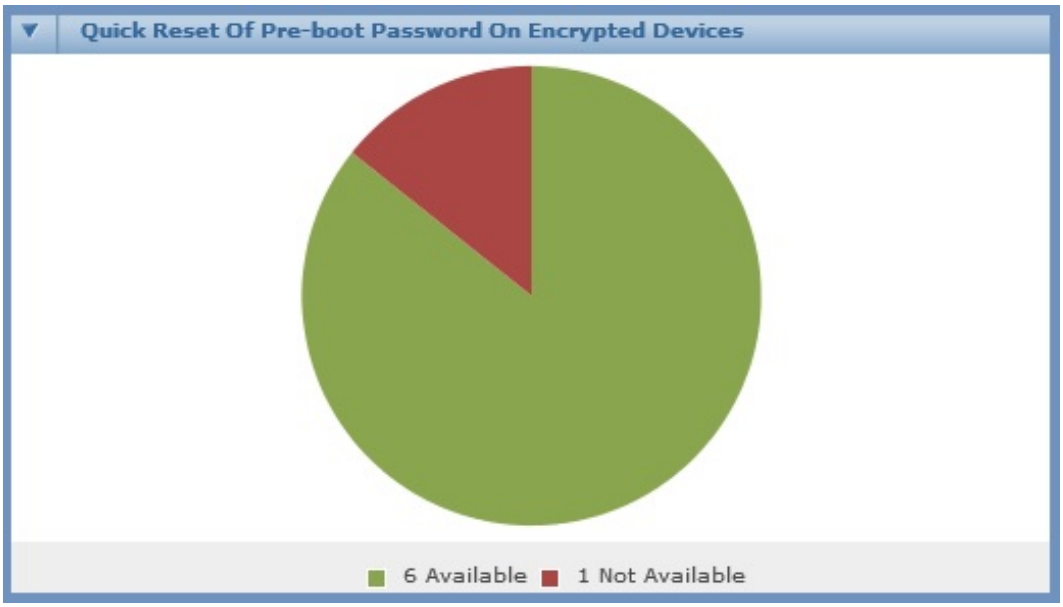
- **Troubleshoot Remote Devices (KVM)** — Displays a pie-chart representing the number of Intel® AMT systems that can be accessed using McAfee KVM to troubleshoot any issues. Systems in this category meet these conditions:
  - Intel® AMT 6.0 or later — installed
  - KVM — supported and enabled
  - Intel® HD Graphics — supported



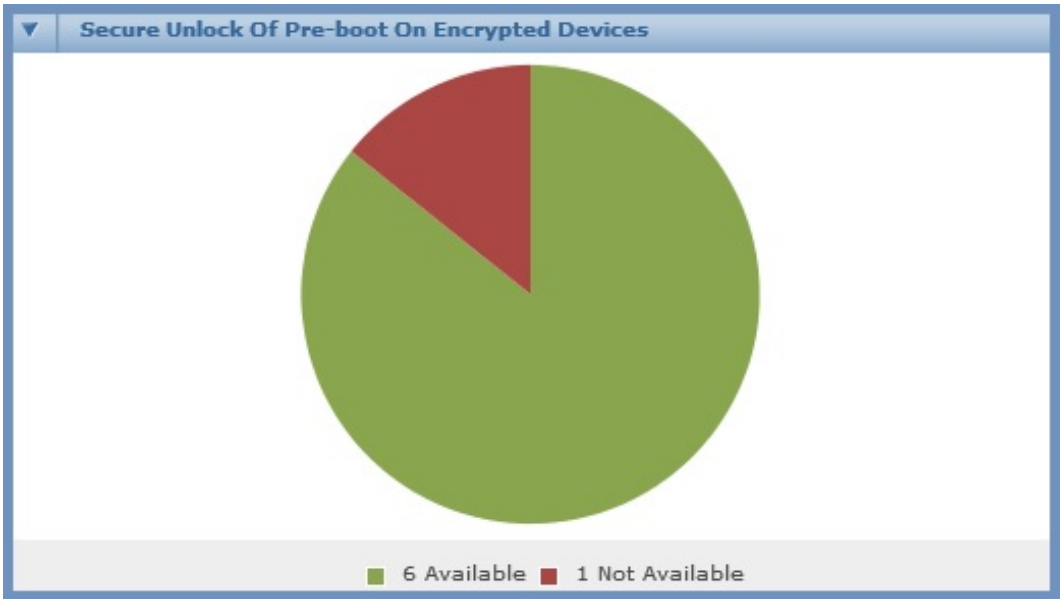
- **Power on remote devices** — Displays a pie-chart representing the number of Intel® AMT systems that can be turned on remotely. Systems in this category have Intel® AMT 4.0 or later.



- **Quick reset of pre-boot password on McAfee encrypted devices** — Displays a pie-chart representing the number of Intel® AMT systems that can reset their pre-boot password using EEPC to regain their access. Systems in this category have Intel® AMT 6.0 or later.



- **Secure unlock of pre-boot on McAfee encrypted devices** — Displays a pie-chart representing the number of Intel® AMT systems that can automatically unlock their pre-boot password using EEPC for device maintenance. Systems in this category have Intel® AMT 6.0 or later.



- **Wake-up devices for security scans and updates** — Displays a pie-chart representing the number of Intel® AMT systems that can automatically update their security signatures and patches. Systems in this category have Intel® AMT 6.0 or later.

ePO Deep Command system properties

When ePO Deep Command components are installed, you can find these properties on the **System Details** page for the managed client systems.

Discovery and Reporting plug-in properties

The Discovery and Reporting plug-in collects properties from the managed systems where it is installed.

The properties that are reported depend on whether the system is an Intel® AMT system, and whether the Intel® MEI driver is installed.

Make sure that **Send full product properties in addition to system properties** is selected in the McAfee Agent policy configuration for the Intel® AMT system. If this option is not selected, the **System Details** page for the client displays no data on the **Deep Command** tab.

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Deep Command tab properties (includes all common properties from **Products** tab)				
Alarm Enabled	Reports whether the ePO Deep Command AMT policy has set the alarm clock in the Intel® AMT firmware.	X		
BIOS Release Date	Reports the release date of the BIOS running on this system using the MM/DD/YY format.	X	X	X
BIOS Version	Reports the version number of the BIOS running on this system.	X	X	X

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
CILA	Reports whether the Client-Initiated Local Access (CILA), also known as Fast Call for Help feature is supported and enabled on this system. This property value is reported as: • **No** • **Not Available** • **Yes**	X		
CILA Agent Handler	Reports the FQDN of the Agent Handler assigned by the ePO Deep Command Remote Access policy to handle CILA requests generated by this system. This property value is reported as: • FQDN of Agent Handler • **Not Available**	X		
CILA Enabled	Reports whether ePO Deep Command Remote Access is enabled and enforced CILA on this system. This property value is reported as: • **No** • **Not Available** • **Yes**	X		
CIRA Enabled	Reports whether the ePO Deep Command Remote Access policy has enabled and enforced Client-Initiated Remote Access (CIRA), also known as Fast Call for Help, on this system. This property value is reported as: • **No** • **Not Available** • **Yes**	X		
CIRA Agent Handler	Reports the FQDN of the DMZ Agent Handler assigned by ePO Deep Command Remote Access policy to handle CIRA requests generated by this system. This property value is reported as • FQDN of DMZ Agent Handler • **Not Available**	X		
Configuration Mode	Reports the configuration mode of this system: • **Enterprise mode** — Enterprise configuration mode	X		
Configuration Mode (TLS)	Reports the TLS configuration mode of this system: • **PKI** — Public Key Interface protocol • **PSK** — Pre-shared Key Based TLS protocol	X		

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Configuration State	Reports the configuration state for this system: • **In-configuration** — The system is being configured. • **Post-configuration** — The system has been configured. • **Pre-configuration** — The system is unconfigured.	X		
DHCP Enabled	Reports whether DHCP is enabled on this system. This property value is reported as **Yes** or **No**.	X		
Endpoint Access Control Enabled	Indicates whether Intel® Endpoint Access Control is enabled to check for Intel® AMT Network Policy Compliance.	X		
Firmware Update Enabled	Reports whether the Firmware Update feature is enabled in the BIOS of this system. This property value is reported as **Yes** or **No**.	X		
Firmware Version	Reports the version number of the Firmware running on this system.	X	X	
Hardware Crypto Enabled	Reports whether the Intel® AMT hardware crypto engine feature is enabled on this system. This property value is reported as **Yes** or **No**.	X		
IDE Redirection (IDE-R)	Reports whether the IDE-R feature is supported and enabled on this system. This property value is reported as: • **Not Available** • **Supported** • **Supported and Enabled** • **Supported and Enabled in BIOS only**	X	X	
Intel® AMT DNS Name	Reports the full Domain Name System name stored in the Intel® AMT firmware on this system. For example, C1amtepo.epoqa.in.	X		
Intel® AMT Fully Configured	Reports whether the Intel® AMT hardware is fully configured. This property value is reported as **Yes** or **No**.	X		
Intel® AMT Supported	Reports whether this system is equipped with Intel® AMT hardware. This property value is reported as **Yes** or **No**.	X	X	
Intel® AMT Version	Reports the version number of the Intel® AMT hardware present on this system. For example, 6.1.20.	X	X	
Intel® Anti-Theft Supported	Reports whether this system supports Intel® Anti-Theft technology. This property value is reported as **Yes** or **No**.	X	X	
Intel® HD Graphic Adapter	Reports whether the system has an Intel® HD Graphic Adapter.	X	X	X
Intel® MEI Enabled	Reports whether the MEI driver is present and turned on. This property value is reported as **Yes** or **No**.	X	X	

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Intel® MEI Version	Reports the version number of the MEI driver running on this system. For example, 6.0.0.1111.	X		
Intel® vPro™ System	Reports whether the target system is an Intel® AMT system. This property value is reported as **Yes** or **No**.	X	X	
Is DNS Configured through DHCP	Reports whether the DNS server of the system is configured through a DHCP server.	X	X	X
Is IDE Redirection Enabled in BIOS	Reports whether IDE-Redirection is enabled in BIOS of the system.	X	X	X
Is IDE Redirection Supported in BIOS	Reports whether IDE-Redirection is supported in BIOS of the system.	X	X	X
Is Intel® AMT FQDN Resolvable from Client	Reports whether the system can resolve its domain name.	X	X	
Is KVM Supported in BIOS	Reports whether KVM is supported in BIOS of the system.	X	X	X
Is Serial-over-LAN Enabled in BIOS	Reports whether SOL is enabled in BIOS of the system.	X	X	X
Is Serial-over-LAN Supported in BIOS	Reports whether SOL is supported in BIOS of the system.	X	X	X
KVM	Reports whether the KVM (Keyboard, Video, and Mouse switch) feature is supported on this system. This property value is reported as: • **Not Available** • **Supported** • **Supported and Enabled** • **Supported and Enabled in BIOS only** This feature is required for using the McAfee KVM Viewer. The Intel® AMT KVM only operates with Intel® Integrated Graphics. It doesn't work on a platform with discrete graphics even if the feature is listed as Supported and Enabled.	X	X	
Last Error Message	Displays the error description for the error that occurred if the last Intel® AMT action failed.	X		
Last IDE-R Session Start/End Time	Reports the time when the last IDE-R session was initiated or stopped. For example, MM/DD/YY 12:00 PM.	X		

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Last IDE-R Session Status	Reports whether the status of the last IDE-R Session was active. This property value is reported as **Yes** or **No**.	X		
Last Power On Success	Reports whether the last attempt to power this system on using Intel® AMT action was successful. This property value is reported as: • **Not Available** • **Yes**	X		
Last Power On Time	Reports the last time this system was powered on as the result of Intel® AMT action. For example, MM/DD/YY 12:00 PM.	X		
Last SOL Session Start/End Time	Reports the time when the last SOL session was initiated or stopped. For example, MM/DD/YY 12:00 PM.	X		
Last SOL Session Status	Reports whether the status of the last SOL Session was active. This property value is reported as **Yes** or **No**.	X		
Local Manageability Service Present	Reports whether the Intel® Local Manageability Service driver is present and turned on. This property value is reported as **Yes** or **No**.	X	X	
Manageability Level	Reports the manageability level for this system. These levels are reported as: • **Full** — Intel® AMT is supported • **None** — Intel® AMT is not supported • **Not Available** — non-Intel® AMT hardware • **Standard** — Intel® AMT is partially enabled	X	X	
Mobile System (Laptop)	Reports whether this system is a laptop. This property value is reported as **Yes** or **No**.	X		
Network Interface Enabled	Reports whether the network interface is enabled on this system. This property value is reported as **Yes** or **No**.	X		
Policy Enforced	Reports whether the ePO Deep Command AMT policy is enforced on this system. This property value is reported as **Yes** or **No**.	X		
Policy Enforcement Time	Displays the last enforcement time for the ePO Deep Command AMT policy on this system. For example, MM/DD/YY 12:00 PM.	X		
Remote Configuration Enabled	Reports whether this system can be configured remotely. This property value is reported as **Yes** or **No**.	X		
Remote Configuration Server	Reports the fully qualified domain name of the configuration server during the configuration. For example, sccm.amtepo.epoqa.in.	X		
Remote Configuration Server IP Address	Reports the IP address of the configuration server during the configuration. For example, 172.12.000.123.	X		

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Reported Local Alarm Clock Time	Displays the alarm clock time set in the Intel® AMT firmware during the ePO Deep Command Alarm Clock policy enforcement or displays **Not available** when no alarm is set.	X		
Serial-over-LAN (SOL)	Reports whether the SOL feature is supported and enabled on this system. This property value is reported as: • **Not Available** • **Supported** • **Supported and Enabled** • **Supported and Enabled in BIOS only**	X	X	
SOL Session Active	Reports whether an SOL session is active on the system.			
System Model	Reports this system's model. For example, Dell OptiPlex 755.	X	X	X
System Manufacturer	Reports this system's manufacturer name. For example, Dell Inc.	X	X	X
System Serial Number	Reports the serial number of this system. For example, 0ABC8BA.	X	X	X
TLS	Reports whether this system is in the Post Configured state with TLS enabled. This property value is reported as: • **Not Available** • **Supported** • **Supported and Enabled** • **Supported and Enabled in BIOS only** This feature must be supported and enabled for ePO Deep Command.	X		
User Consent Mode Required	Reports whether the user consent is required for applying Intel® AMT actions on this system.	X		
UUID	Reports the ID for this systems hardware. For example, 4C4C4D44-004A-4A10-8048-C4C44F384253.	X	X	X
Web UI Enabled	Reports whether the Intel® AMT web interface is enabled on this system (during the configuration). This property value is reported as **Yes** or **No**.	X		
Wired IPv4 Address	Reports the IPv4 address received over this system's physical network connection. For example, 172.12.000.123.	X		
Wired Link Status	Reports whether this system's physical network connection is functioning. This property value is reported as **Up** or **Down**.	X		
Wired MAC Address	Reports the MAC address received over this system's physical network connection. For example, 781bcb8cf20a.	X		

Property	Description	With Intel® MEI driver installed	Without Intel® MEI driver installed	Non-Intel® AMT System
Wireless IPv4 Address	Reports the IPv4 address received over this system's wireless network connection. For example, 172.12.000.123.	X		
Wireless Link Status	Reports whether this system's wireless network connection is functioning. This property value is reported as Up or Down.	X		
Wireless MAC Address	Reports the MAC address received over this system's wireless network connection. For example, 781bcb8cf20a.	X		
Extra properties under **Products** | **McAfee ePO Deep Command Detection Plugin**				
McAfee ePO Deep Command Detection Plugin	Displays **AMTDET** as the plug-in name.			
Product Version	Displays the version of the Discovery and Reporting plug-in.			
System Time Bias	Displays the difference between the system time and actual time based on the existing location of the system.			
Installed Directory	Displays the directory path where the Discovery and Reporting plug-in is installed.			
Language	Displays the language of the Discovery and Reporting plug-in. The current release is available only in English language.			
Language ID	Displays the ID of the Discovery and Reporting plug-in language. The current release is available only in English language.			

Management Framework client properties

When ePO Deep Command client is installed on an Intel® AMT system, these properties appear in the **Products** tab on the **System Details** page for the client.

Option	Definition
General Properties	
McAfee ePO Deep Command Client	Displays **AMT** as the client name.
Product Version	Displays the ePO Deep Command client version installed on the system.
Language	Displays **Neutral** because localized language options are not available with the current release.
Hotfix/Patch Version	Displays the ePO Deep Command hotfix or patch release version, if applicable.
Service Pack	Displays the ePO Deep Command Service Pack version, if applicable.
Deep Command Management Properties	
Configuration Profile	Displays the name of the configuration profile used in configuring the Intel® AMT systems.
Control Mode	Displays the current configuration mode of the Intel® AMT system: **Client Control Mode**, **Admin Control Mode**, or **Unconfigured**.

Option	Definition
Host-Based Configuration	Whether host-based configuration is supported on the client: **Supported** or **Not Supported**.
Is Embedded HBC Enabled	Whether host-based configuration is enabled.
RCS Server	Displays the Intel® RCS server name if the client is in Admin Control mode.

RCS Management plug-in properties

The RCS Management plug-in collects properties from the managed Intel® RCS systems where it is installed.

Property	Definition
General Properties	
McAfee ePO Deep Command RCS Manager Plugin	Displays the **AMTRCS** as the plug-in name.
Product Version	Displays the version of the ePO Deep Command client.
Installed Directory	Displays the directory path where the ePO Deep Command RCS Manager plug-in is installed.
Language	Displays the language of the ePO Deep Command RCS Manager plug-in. The current release is available only in English language.
Profile Properties	
Digest Master Password Set	Whether the Intel® RCS server profile is configured to use a Digest Master Password.
Network Timeout (seconds)	Displays the time set for which the Intel® RCS tries to establish a connection.
Profile Names	Displays the configuration profiles configured on the Intel® RCS server.

8 Managing your Intel AMT systems

Manage the Intel® AMT systems in your network by using Intel® AMT policies, client task execution policies, Intel® AMT actions, server tasks, and queries.

Contents

- *Using policies to manage Intel AMT systems*
- *Create the Profile Manager policies*
- *Use the Intel AMT actions*
- *Automate Intel AMT policy enforcement*
- *Maintenance tasks*
- *Managing events and logs*

Using policies to manage Intel AMT systems

Policies ensure that the product features are configured correctly, while client tasks are the scheduled actions that run on the managed systems hosting any client-side software.

When you change a policy from McAfee ePO, that policy is enforced at the next agent-server communication. As a result, the next time a system that has received the new policy is turned on, the new policy is enforced automatically.

ePO Deep Command has these policies:

- In-band — Allows performing agent-based operations using the ePO Deep Command client agent.
  - Client Task Execution policy
  - AMT Configuration policy
- Out-of-band — Allows performing Intel® AMT actions.
  - Alarm Clock policy
  - Remote Access policy
  - Local Access policy
  - KVM policy

Create the Intel AMT configuration policies

Use the **AMT Configuration Policies** category to create policies to configure or unconfigure your Intel® AMT systems.

Tasks

- *Create a policy to configure Intel AMT systems* on page 94
  You can create a policy based on the Intel® AMT configuration policies.
- *Create a policy to unconfigure Intel AMT systems* on page 94
  You can create an unconfigure policy based on the Intel® AMT configuration policies.
- *Move systems from Client Control to Admin Control mode* on page 95
  Move Intel® AMT systems that were configured using host-based configuration to run in Admin Control mode.

Create a policy to configure Intel AMT systems

You can create a policy based on the Intel® AMT configuration policies.

Before you begin
For Remote Configuration, make sure that the ePO Deep Command Profile Manager software is installed and configured.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Select **Allow ePO to enforce these settings**, then select appropriate options.

- **Remote configure to enable Admin Control Mode** — Select for remote configuration, then select the Intel® RCS server and the profile to be used for the configuration.
- **Host based configure to enable Client Control Mode** — Select for host-based configuration, then select the host-based profile. This configuration method doesn't need a configuration server.

4 Save the policy.

See also

Configuring Intel AMT systems on page 4

Create a policy to unconfigure Intel AMT systems

You can create an unconfigure policy based on the Intel® AMT configuration policies.

Before you begin
For the client in Admin Control mode, make sure that the ePO Deep Command Profile Manager software is installed and configured.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Select **Allow ePO to enforce these settings**, then perform one of these steps based on configuration mode of systems.

- **Admin Control mode** — Select **Remote configure to enable Admin Control Mode**, select **Unconfigure (if currently configured by ePO)**, and then select the Intel® RCS server and profile used for the configuration.
- **Client Control mode** — Select **Host-based configure to enable Client Control Mode**, select **Unconfigure (if currently configured by ePO)**, and then select the profile used for the configuration. The Intel® AMT systems in this mode do not require an Intel® RCS server. They use the host-based profile to configure or unconfigure the client.

4 Select the appropriate unconfigure options.

- **Also remove the pre-shared keys or hash data of self-signed CA certificates configured on the client systems manually.** — Removes the configuration completely.
- **Force unconfigure even if it is not configured by ePO** — Removes the configuration from a system that was not configured using McAfee ePO.

5 Save the policy.

See also

Unconfigure Intel AMT systems through McAfee ePO on page 54

Move systems from Client Control to Admin Control mode

Move Intel® AMT systems that were configured using host-based configuration to run in Admin Control mode.

Before you begin

Make sure that the Intel® AMT systems meet the requirements and prerequisites for Admin Control mode. See *Requirements and Prerequisites* for remote configuration.

When you configure your Intel® AMT systems using the host-based configuration, the system is automatically placed in Client Control mode that has limited access. However, you can move your systems to run in Admin Control mode.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Configuration Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Select **Allow ePO to enforce these settings**, select **Remote configure to enable Admin Control Mode**, select **Move to Admin Control Mode if currently in Client Control Mode**, then select the Intel® RCS server and profile to be used for the configuration.

Make sure to select the required profile. By default, the first profile in the list is used.

4 Save the policy.

When this policy is enforced, the Intel® AMT systems in Client Control mode are unconfigured, then configured again using remote configuration. Intel® AMT policy is enforced on the clients to synchronize data. See **Server Task Log** for the policy status.

Create the Intel AMT policies

Use the **AMT Policies** category to create a policy to turn on your Intel® AMT systems, configure Local Access or Remote Access for technical assistance, and set McAfee KVM Viewer preferences.

You can also create separate policies for each feature. For better clarity on each feature, we have provided separate tasks for each feature. However, we recommend that you define Alarm Clock, Local Access, and Remote Access settings in a single policy and assign it to the required systems or groups.

Tasks

- *Create an Alarm Clock policy* on page 96
  The Alarm Clock feature enables you to remotely schedule to turn on Intel® AMT systems at a defined time and perform specific tasks.
- *Create a Local Access policy* on page 97
  The Local Access feature allows the local Intel® AMT system to initiate a Fast Call For Help inside the enterprise network.
- *Create a Remote Access policy* on page 98
  Initiate a secured connection from McAfee ePO to remote Intel® AMT systems through Gateway server.
- *Create a KVM policy* on page 100
  McAfee KVM Viewer provides a console to access remote clients. It can be used to access an Intel® AMT system for troubleshooting any issues.

See also

Supported Intel® AMT versions on page 20

Create an Alarm Clock policy

The Alarm Clock feature enables you to remotely schedule to turn on Intel® AMT systems at a defined time and perform specific tasks.

Consider these points:

- The time you set is based on the location of your Intel® AMT system. If you specify the Alarm Clock time to be fewer than five minutes of the current time of your Intel® AMT system, the policy enforces the Alarm Clock Time for the next day.
- When you move from one time zone to another, the Intel® AMT system might turn on at a time not in sync with the local time. This issue can be resolved after the next agent-server communication or by modifying and enforcing the policy manually.
- The required tasks can be performed during off-hours to avoid interrupting the Intel® AMT systems users.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Policies** as the category, then click **New Policy**.
2. Type a name for the policy and any notes, then click **OK**.
3. Click the policy created, then select **Allow ePO to enforce these settings**.
4. Enable the Alarm Clock at a particular time and specify the randomization minutes.

   Randomization minutes balances the policy distribution to selected Intel® AMT systems. The maximum value is 20 minutes.

5 Select **Repeat Every** to specify the days, hours, and minutes to turn on your systems at regular intervals, then save the policy.

6 In the **System Tree**, assign the policy to the required systems or group.

- **Systems** — Click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Policies** as the category, select the modified policy, select **Break Inheritance**, then save the policy assignment.
- **Group** — Select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Policies**, select the modified policy under **Assigned policy**, then save the policy assignment.

7 Enforce the policy using one of these methods:

- Wait for the next agent-server communication.
- Send an agent wake-up call.
- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
- Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

8 Verify the policy enforcement:

- View the policy enforcement status in **Server Task Log**.
- Navigate to the **System Properties** page, click the **Deep Command** tab, and make sure that the alarm is updated in the **Reported Local Alarm Clock Time**.
- In the amtservice.log, the policy enforcement status is successful and the Alarm Clock Set Time is shown in Universal Time Coordinated (UTC).

See also

Enforce Intel AMT policies on page 111

Create a Local Access policy

The Local Access feature allows the local Intel® AMT system to initiate a Fast Call For Help inside the enterprise network.

> **Before you begin**
> The Local Area Network (LAN) Agent Handler to be used for the Local Access policy must be active.

When a user initiates a connection, Intel® AMT detects that it is inside the enterprise and sends a local access request directly to McAfee ePO.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Click the policy created, click the **Remote Access** tab, then select **Allow ePO to enforce these settings**.

4 From the **Local Server**, select **Enable Client Initiated Local Access (CILA)**, then select an active LAN Agent Handler from the drop-down list.

5 In **Connection Type**, select where the Intel® AMT system initiates the call to McAfee ePO. Available options are **BIOS Initiated** and **OS Initiated**.

6 Click **Save**.

7 In the **System Tree**, assign the policy to the required systems or group.

- **Systems** — Select the systems, click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Policies** as the category, select the modified policy, select **Break Inheritance**, then save the policy assignment.
- **Groups** — Select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Policies**, select the modified policy under **Assigned policy**, then save the policy assignment.

8 Enforce the policy using one of these methods:

- Wait for the next agent-server communication.
- Send an agent wake-up call.
- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
- Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

9 Verify the policy enforcement:

- View the policy enforcement status in **Server Task Log**.
- Navigate to the **System Properties** page, click the **Deep Command** tab, and make sure that the value for **CILA Enabled** is **Yes** and the Agent Handler you selected is listed under **CILA Agent Handler**.
- Initiate a call from the Intel® AMT system using the **Get Technical Help** option in the Intel® Management and Security Status tool. The IMSS tool indicates whether the system is connected. After this action, the **Threat Event Log** on McAfee ePO displays an entry for the **Local Fast Call for Help** log with an event ID 34350.

See also

Enforce Intel AMT policies on page 111

Create a Remote Access policy

Initiate a secured connection from McAfee ePO to remote Intel® AMT systems through Gateway server.

Before you begin

- McAfee ePO Agent Handler 4.6 Patch 4 must be installed on the ePO Deep Command Gateway server DMZ and must be active.
- The FQDN of the ePO Deep Command Gateway server must be resolvable from the Internet.
- The Remote Access configuration ports must be allowed through the DMZ firewall and be accessible to the remote Intel® AMT system clients. Usually, this port is where stunnel is configured.
- Stunnel version 4.36 or later must be installed on the Agent Handler servers.

Remote Access is an advanced feature of Intel® AMT technology platforms that initiates a secured connection from your server to the Intel® AMT systems through a gateway server residing in the enterprise DMZ. Make sure that you provide the correct details of your Intel® AMT system environment while configuring a Remote Access policy. If there's a mistake, especially while enforcing the Remote Access policy to a larger environment, you might need to be physically present to unconfigure each Intel® AMT system, then reconfigure them.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Click the policy created, click the **Remote Access** tab, then select **Allow ePO to enforce these settings**.

4 In **Remote Server**, select **Enable Client Initiated Remote Access (CIRA)**.

5 In **Home Domain Suffix**, type the host name of the Intel® AMT systems, then click **Add**.

Adding home domain suffixes enables the Intel® AMT systems to access the home domains. The home domain refers to the detected DHCP 15 value of the network, that is, Connection Specific DNS suffix, using which Intel® AMT determines if a system is inside or outside the environment. The Intel® AMT system must be outside the enterprise. You must enter at least one home domain suffix. You can enter a maximum of 5 home domain suffixes.

The DHCP and DNS servers must be configured for successful execution of the Remote Access policy. The details you specify in this step must match your connection-specific DNS suffixes in your LAN. Incorrect home domain suffix settings might turn off the access to the Intel® AMT systems unless a Remote Access session is established by the system itself.

6 Select a primary DMZ Agent Handler and specify the stunnel port (as specified in the stunnel configuration) for the incoming Remote Access requests.

7 In **Tunnel Lifetime**, specify the time (in seconds) the Remote Access tunnel must be active after it is established.

The default value is zero, which sets the connection to no timeout.

8 Select these options:

- **Allow User Initiated Tunnel** — Allows Intel® AMT users to initiate a Remote Access request to the server.
- **Periodic Initiated Tunnel every** — Specifies a time to establish the connection at regular intervals.

9 In **Connection Type**, select where the Intel® AMT system initiates the call to McAfee ePO. Available options are **BIOS Initiated** and **OS Initiated**.

10 Click **Save**.

11 In the **System Tree**, assign the policy to the required systems or group.

- To assign the policy to selected systems, select the systems, click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Policies** as the category, select the modified policy, select **Break Inheritance**, then save the policy assignment.
- To assign the policy to a system group, select the group, select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Policies**, select the modified policy under **Assigned policy**, then save the policy assignment.

12 Enforce the policy using one of these methods:

- Wait for the next agent-server communication.
- Send an agent wake-up call.

- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
- Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

13 Verify the policy enforcement:

- View the policy enforcement status in **Server Task Log**.
- Navigate to the **System Properties** page, click the **Deep Command** tab, make sure that the value for **CIRA Agent Handler** is **Yes** and the Agent Handler you selected is listed under **CILA Agent Handler**.
- Initiate a call from the Intel® AMT system using the **Get Technical Help** option in the Intel® Management and Security Status (IMSS) tool. The IMSS tool indicates whether the system is connected. This is part of the environment detection indicator as defined by the **Home Domains** setting. After this action, the **Threat Event Log** logs an entry for the **Remote Fast Call for Help** log with an event ID 34351.

See also

Setting up your environment for Remote Access on page 4
Enforce Intel AMT policies on page 111

Create a KVM policy

McAfee KVM Viewer provides a console to access remote clients. It can be used to access an Intel® AMT system for troubleshooting any issues.

Before you begin

Correct Intel® AMT credentials must be set, and a trusted root certificate must be uploaded in the **Server Settings** page for the **Intel® AMT Credentials** category.

You can configure this policy to enable or disable KVM feature, user's consent for the connection, opt in timeout, session timeout and more.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **AMT Policies** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Click the policy created, click the **KVM Settings** tab, then select **Allow ePO to enforce these settings**.

4 In **KVM State and Ports Used**, select **Enable with TLS on Port 16995**, then select **Enable Opt-In** to specify whether user's consent is required for every connection (optional) and type the **Opt-In timeout** in seconds to specify the time after which the passcode for the user's consent is expired if no connection is established.

When you use the KVM Viewer for an Intel® AMT system that was configured using the host-based configuration, the User Consent mode is enabled by default, even if the **Opt-in** option is disabled in the policy enforced.

5 In **Default Visible Monitor**, select which monitor of the client system to display (if the client has multiple monitors): **Primary**, **Secondary**, or **Tertiary**.

6 In **TCP Session Timeout**, type the number of minutes after which the session times out, then save the policy.

7 In the **System Tree**, assign the policy to the required systems or group.
   - To assign the policy to selected systems, select the systems, click **Actions** | **Agent** | **Set Policies & Inheritance**, select **ePO Deep Command 2.1** as the product, select **AMT Policies** as the category, select the modified policy, select **Break Inheritance**, then save the policy assignment.
   - To assign the policy to a system group, select the group, select **ePO Deep Command 2.1** as the product, click **Edit Assignment** next to **AMT Policies**, select the modified policy under **Assigned policy**, then save the policy assignment.

8 Enforce the policy using one of these methods:
   - Wait for the next agent-server communication.
   - Send an agent wake-up call.
   - From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.
   - Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

9 View the policy enforcement status in **Server Task Log**.

See also

Connecting to Intel AMT systems using KVM on page 5

Creating the Client Task Execution policy

Enforcing the **Client Task Execution** policies to the Intel® AMT systems executes the client tasks, the arbitrary command, and other parameters when powered on through McAfee ePO.

Create a Client Task Execution policy

Create a policy to execute a client task from the **Policy Catalog**, then assign it to the required client systems.

Before you begin

Make sure that:

- Client Tasks feature is enabled for the Intel® AMT system.
- Required managed products are installed on the Intel® AMT system.
- The Intel® AMT system can be started using the Power On action or Alarm Clock task.
- There's no delay in starting Intel® AMT system using the Power On action or Alarm Clock task, and in further communication.
- The Intel® AMT system is not in a state of hibernation or standby.
- The assigned task must have been successfully run at least once on the Intel® AMT system.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command 2.1.0** as the product and **Client Task Execution** as the category, then click **New Policy**.

2 Type a name for the policy and any notes, then click **OK**.

3 Click the policy created to configure it.

4 In **Run the following Command afterward (optional)**, select the product, task type, and client tasks.

Client tasks that require a system restart must be added last in the sequence.

5 In **When to execute client task**, select **Execute the task only when system boots due to Alarm clock** to avoid executing it when the system starts due to Power on action.

6 (Optional) In **Run the following Command afterwards**, add the arbitrary command, and its parameters to execute it after the client task.

For example, the command `<System32>\shutdown.exe` shuts down your system after the client task is run. You can also add parameters for the command that you type. If you add `/h`, the Intel® AMT system enters the hibernate mode, and if you add `/r`, it restarts.

7 Click **Save**.

8 In the **System Tree**, select the systems, click the **Assigned Client Tasks** tab, then create a client task assignment to assign the client tasks added to the **Client Task Execution** policy as in step 2.

9 In the **System Tree**, select the systems, click the **Assigned Policies** tab, click **Edit Assignment** next to the **Client Task Execution** policy created or modified in the step 1, then save the assignment.

10 Enforce the policy using one of these methods:

- Wait for the next agent-server communication.
- Send an agent wake-up call.
- From the Intel® AMT systems, click **McAfee Agent Status Monitor**, then click **Collect and Send Properties**, **Check New Policies**, and **Enforce Policies**.

Client Task Execution policy logs and services

These logs and services are displayed on the Intel® AMT system.

Log files and services

Based on the platform, you'll find the log files under these directories on an Intel® AMT system:

- **For systems running on Microsoft Windows XP and Microsoft Windows Server 2003** — `..\Documents and Settings\Default User\Application Data\McAfee`
- **For systems running on other operating systems** — `..\ProgramData\McAfee\ePO Deep Command Client`

Log files	Description
AMTMgmtService_out.log	Log file that provides the details of client tasks scheduled in an Alarm Clock policy. The information includes the Client Task Execution policy and the message status.
AMTCT_out.log	Log file that displays the status of client tasks executed using Alarm Clock policies.
AMTCT.exe	This service starts and sequentially executes the client task, specified arbitrary command, and its additional parameters, as defined in the Alarm Clock policy. The information include the Client Task ID, software ID, and arbitrary command if present.

Compare ePO Deep Command policies

In McAfee ePO 5.0, you can compare two policies under the same category.

For detailed information on the **Policy Comparison** feature, see the McAfee ePO 5.0 product documentation.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Policy Comparison**, select **ePO Deep Command 2.1.0** or **ePO Deep Command Profile Manager 2.1.0** as the product, select a policy category, then select **All Policy Settings**.

2 Select the policies to compare in the **Compare policies** row from the **Policy 1** and the **Policy 2** column lists.

List of settings available in the policy and their values appear for the comparison.

Create the Profile Manager policies

Use the **Profile Manager** category to create or import an Intel® AMT profile and to provide timeout for a remote connection.

Tasks

- *Create a Configuration Profile policy* on page 103
  Create a policy to create or import a configuration profile for Intel® AMT systems.
- *Set the time-out for remote system* on page 105
  When you use remote configuration, create this policy to specify the time (in seconds) for which the Intel® RCS to establish a connection.

Create a Configuration Profile policy

Create a policy to create or import a configuration profile for Intel® AMT systems.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, navigate to **Policy Catalog**, select **ePO Deep Command Profile Manager 2.1.0** as the product and **Configuration Profile** as the category, then click **New Policy**.

2 Select **McAfee Default**, type a name for the configuration policy and any notes, then click **OK**.

3 In the **General** tab,

a Type a description for the profile.

b Select a profile template:

- **Default** — Use a default template: **Remote configuration with TLS** or **Host base configuration with TLS**.
- **User** — Use a custom template that you imported. To import a new custom template, click **Import**, then

1 Browse to select a template exported from Intel® RCS console.

2 Type a name for the template.

3 Type the password to decrypt the template.

You can only import a password encrypted profile.

4 Retype the password to confirm, then click **OK**.

c Type the Intel® MEBX password, then retype it to confirm.

Select **Show Password** to see the password as you type. Password confirmation is not required with this option.

This step can be used only for a remote configuration template.

d Select **Use generated random password** to use a randomly generated digest password or select **set password**, type a digest password, then retype it to confirm.

Select **Show Password** to see the password as you type. Password confirmation is not required with this option.

The password must match the Intel® AMT credentials entered in **Server Settings**.

e (Optional) Select **Integrate with Active Directory**, then browse to select the Active Directory Organization Units.

f In **AMT User accounts and rights**, perform one of these steps:

- For Digest account, click **New Digest User**, type user name, type password, retype password (or select **Show Password**), then select the required access right for the use:
  - **Administrator** — Provides PT Administration rights, which allows the user to access all Intel® AMT features. A PT Administrator manages security control data such as Access Control Lists, Kerberos parameters, Transport Layer Security, Configuration parameters, power-saving options, and power packages. Also this user has access to all realms.

    If a PT Administrator wants to run configurator to perform host-based configuration, the **Access Type** must be selected as **Local** or **Both**.

  - **Help Desk** — Provides these access rights:
    - **Hardware Asset** — To retrieve information about the hardware inventory of the Intel® AMT system.
    - **Storage** — To configure, and write to and read from non-volatile user storage.
    - **General Info** — To retrieve general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters.
    - **Endpoint Access Control** — To retrieve settings associated with NAC/NAP posture.
    - **Event Log Reader** — To allow definition of a user with permissions only to read the Intel® AMT system log.
    - **User Access Control** — To group ACL management commands into a separate realm to enable users to manage their own passwords without requiring administrator rights.
  - **Remote Power Control** — Provides these access rights:
    - **Redirection** — To enable and disable the redirection capability and retrieves the redirection log.
    - **Remote Control** — To enable powering up a system or shutting it down remotely. Used with the Redirection capability to boot remotely.
    - **General Info** — To retrieve general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters.
  - (Optional) To modify a saved digest account, select it, then click **Edit**.

- For Kerberos account,
  1. Select **New Kerberos User** or **New Kerberos Group**, as needed, select the required user or group, then click **OK**.
  2. Select the user or group, then select the required access right for the user or group (**AMT Administrator**, **AMT Help Desk**, **AMT Remote Power Control**).

4. (Optional) In the **Advanced** tab, complete these Remote configuration options:
   - **Remote management** — Select whether to enable the web interface for Intel® AMT management.
   - **Intel Fast Call for Help** — Select when a user can initiate a call for help:
     - **OS initiated** — from the operating system.
     - **BIOS initiated** — from the BIOS.
   - **IP address** — Select the source for the IP address settings:
     - **DHCP** — from the DHCP server.
     - **Static** — the same IP address as the host.
   - **FQDN** — Select the source for the host name suffix:
     - **Primary DNS** — from the "Primary DNS Suffix" of the host operating system.
     - **Active directory name** — from the Active Directory domain where the host operating system is a member.

   These options can be used only for a remote configuration template.

5. Save the policy.

Set the time-out for remote system

When you use remote configuration, create this policy to specify the time (in seconds) for which the Intel® RCS to establish a connection.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **Policy Catalog**, select **ePO Deep Command Profile Manager 2.1.0** as the product and **Remote Configuration Services Policies** as the category, then click **New Policy**.
2. In **Timeout for connection with systems**, type the number of seconds for which the Intel® RCS to establish a connection.
3. Save the policy.

Use the Intel AMT actions

You can create and enforce actions on your configured remote Intel® AMT systems.

Before you begin
In the **System Tree**, verify that your managed systems have the **AMT** tag assigned to them.

When Intel® AMT actions are performed over a wireless connection, the host operating system loses the connection while the Intel® MEI is executing it. Once the action is complete, the host operating system regains the connection.

Tasks

- *Turn on your systems* on page 106
  The Power On feature allows your Intel® AMT systems to deploy the updated security programs ahead of a potential threat outbreak.
- *Obtain User Consent* on page 107
  Obtain User Consent to perform Intel® AMT actions using a passcode generated on the Intel® AMT system screen to connect.
- *Boot or restart to BIOS* on page 107
  BIOS is the boot firmware program that controls your system from the time it starts until operating system takes over.
- *Boot or restart a system normally* on page 108
  You can boot or restart the managed Intel® AMT systems from McAfee ePO when required. For example, when you want to leave the recovery operating system image.
- *Connect to a system using the Serial-over-LAN* on page 109
  Serial-over-LAN (SOL) is a mechanism that enables the input and output of the serial COM port of a managed Intel® AMT system to be redirected over Internet Protocol (IP address).
- *Boot or restart using IDE-Redirection* on page 109
  IDE-Redirection allows you to restart an Intel® AMT system to a redirected disk.
- *Stop image redirection* on page 111
  You can stop an in-progress image redirection for the selected client systems, as needed.
- *Enforce Intel AMT configuration policy* on page 111
  You can use this action to immediately configure the Intel® AMT capable systems that have a configuration policy assigned to them.
- *Enforce Intel AMT policies* on page 111
  You can use this action to immediately enforce the Intel® AMT policies of Alarm Clock, Local Access, Remote Access, and KVM, on the selected systems.

Turn on your systems

The Power On feature allows your Intel® AMT systems to deploy the updated security programs ahead of a potential threat outbreak.

Before you begin

- Correct Intel® AMT credentials must be set, and a trusted root certificate must be uploaded in the **Server Settings** page.
- The Intel® AMT systems must be configured.
- A power cable must be connected to the Intel® AMT systems, including laptops.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Systems** | **System Tree**.

2 Select the required systems or groups that you want to turn on.

3 Click **Actions** | **AMT Actions** | **Power On**, then click **OK**.

4 View the policy enforcement status in **Server Task Log**.

Obtain User Consent

Obtain User Consent to perform Intel® AMT actions using a passcode generated on the Intel® AMT system screen to connect.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **System Tree**, select a system, which is in Client Control mode.

2 Click **Actions** | **AMT Actions** | **Get User Consent**.

User Consent status of the selected client system is displayed.

- **User Consent is needed and not yet started** — The selected system is in Client Control mode and requires User Consent.
- **User Consent is now displayed on client system** — User Consent code has been generated and displayed on the client screen. Skip steps 3–5.
- **User Consent is already obtained and it is currently in progress** — The code has been validated and User Consent mode is in-progress. Skip steps 3–6.

3 Type the timeout for UCM code. This time specifies the number of seconds to wait before the UCM code is displayed. When the Intel® AMT system is in hibernate mode or is powered off, then the ePO Deep Command client first turns on the system.

4 Select the monitor of the Intel® client system to display: **Primary**, **Secondary**, or **Tertiary**.

5 Click **Start** to generate a UCM code.

6 Type the code, then click **Send Code**.

7 When the required action has been performed, click **Stop** to end the UCM session, then click **Cancel** to close the **User Consent** page.

Boot or restart to BIOS

BIOS is the boot firmware program that controls your system from the time it starts until operating system takes over.

Boot or restart your Intel® AMT system to BIOS to diagnose issues. Use the SOL option to access the Intel® AMT system from the server during system diagnosis. You can also perform this task from the McAfee KVM Viewer console.

For Intel® AMT 7.0 systems, establish the SOL connection before initiating the **Boot/Reboot to BIOS Setup** action to get a full screen refresh in the SOL terminal.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **System Tree**, select the systems you want to diagnose by starting them up to their BIOS.

2 Click **Actions** | **AMT Actions** | **Boot/Reboot with Options**.

3 In **Actions**, select **Boot/Reboot to BIOS Setup** to boot or restart to the BIOS of the crashed Intel® AMT system, and diagnose issues by adjusting its BIOS settings.

4 (Optional) In **Additional Action**, select **Launch Serial-over-LAN Terminal (SOL)** to access the target system from the server side.

You can use the arrow keys to navigate through the BIOS menu that is displayed on the SOL terminal.

5 In **User Consent Mode**,

a Select **Operate in User Consent Mode (UCM)**.

Make sure that you enable the User Consent Mode for only one system at a time. User consent is required for the clients in Client Control mode and optional for the clients in Admin Control mode.

b Type the timeout for UCM code. This time specifies the number of seconds to wait before the UCM code is displayed. When the Intel® AMT system is in hibernate mode or is powered off, then the ePO Deep Command client first turns on the system.

c Select the monitor of the Intel® client system to display: **Primary**, **Secondary**, or **Tertiary**.

d Click **Start UCM** to generate a UCM code on the Intel® AMT system, then type the code displayed on the client system.

6 Click **Initiate Action** to establish the connection and initiate the required action.

7 View the policy enforcement status in **Server Task Log**.

When the **Boot/Reboot with Options** status is **In Progress**, a connection is established and you can start diagnosing the system issues.

See also

Connect to a system using the Serial-over-LAN on page 109
McAfee KVM Viewer options on page 127

Boot or restart a system normally

You can boot or restart the managed Intel® AMT systems from McAfee ePO when required. For example, when you want to leave the recovery operating system image.

You can also perform this task from the McAfee KVM Viewer console.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **System Tree**, select the systems that you want to boot or restart.

2 Click **Actions** | **AMT Actions** | **Boot/Reboot with Options**.

3 Select **Normal Boot/Reboot** to boot or restart the Intel® AMT system. You can also select **Launch Serial-over-LAN Terminal (SOL)** to access the Intel® AMT system from the server side.

4 View the policy enforcement status in **Server Task Log**.

See also

McAfee KVM Viewer options on page 127

Connect to a system using the Serial-over-LAN

Serial-over-LAN (SOL) is a mechanism that enables the input and output of the serial COM port of a managed Intel® AMT system to be redirected over Internet Protocol (IP address).

Before you begin

- Make sure that SOL is supported and enabled on your Intel® AMT systems. Verify this from the **Deep Command** tab on the **System Properties** page.
- Make sure that the correct Intel® AMT credentials are set, and a trusted root certificate is uploaded on the **Server Settings** page.
- Make sure to enforce the Intel® AMT policies on systems where you are attempting to establish an SOL connection.
- Make sure that the Intel® AMT system is accessible from the Agent Handler and the port 16995 is not blocked in the firewall.
- Make sure that **Console Redirection** is enabled in BIOS setup. This feature is enabled automatically as part of Intel® AMT policy enforcement. However, for some manufacturers, you must enable this feature manually.

You can use SOL to connect to a remote Intel® AMT system through a virtual serial port. After initiating an SOL session, you can see it is active. You can also access the BIOS of the Intel® AMT system and send keyboard key combinations using SOL.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **System Tree**, select up to four systems, which you want to connect using SOL.

SOL is processed on a maximum of four systems at one time per Agent Handler.

2 Click **Actions** | **AMT Actions** | **Serial-Over-LAN Terminal (SOL)** to display the SOL terminal.

3 Click **Connect** to start a connection with the selected system. When the **Terminal <=> ePO: Connected** message appears, the SOL session is active.

The screen is blank if the serial port has not sent any data, even though connection is established. You can send keyboard key combinations to the Intel® AMT systems. These keys are specific to the terminals. For example, If **Ctrl-C** is the key that stops the ping command on a Linux terminal, selecting and sending this key to the Linux terminal by clicking **Send** on the SOL Terminal stops the ping command.

4 View the policy enforcement status in **Server Task Log**.

Boot or restart using IDE-Redirection

IDE-Redirection allows you to restart an Intel® AMT system to a redirected disk.

Before you begin

- IDE-Redirection must be supported and enabled on the Intel® AMT systems. Verify this from the **Deep Command** tab on the **System Properties** page.
- You must have enforced Intel® AMT policies at least once on the target systems to enable the redirection port.

- The recovery operating system image file must be an .iso file shared on a UNC mount. It must be shared and accessible by the Agent Handler. Also, make sure that you have defined its path using the Universal Naming Convention (UNC) syntax rather than using the IP address.
- Make sure that the image file can be used for diagnosis, and its size is smaller than 30 MB.

If your ISO image is larger than 30 MB, or you have network bandwidth constraints, see this document for more information about using a two stage boot process: http://communities.intel.com/docs/DOC-5552.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **System Tree**, select up to four systems, which you want to diagnose using the IDE-Redirection feature.

IDE-Redirection is processed on a maximum of four systems at one time per Agent Handler.

2 Click **Actions** | **AMT Actions** | **Boot/Reboot with Options**.

3 Select **Boot/Reboot from Image (IDE-R)** to boot or restart the target Intel® AMT system using a recovery operating system image (.iso file) to diagnose issues. Type the path of the recovery operating system image file.

4 (Optional) In **Additional Action**, select **Launch Serial-over-LAN Terminal (SOL)** to access the target system from the server side.

You can use the arrow keys to navigate through the BIOS menu that is displayed on the SOL terminal.

5 In **User Consent Mode**,

a Select **Operate in User Consent Mode (UCM)**.

Make sure that you enable the User Consent Mode for only one system at a time. User consent is required for the clients in Client Control mode, and optional for the clients in Admin Control mode.

b Type the timeout for UCM code. This time specifies the number of seconds to wait before the UCM code is displayed. When the Intel® AMT system is in hibernate mode or is powered off, then the ePO Deep Command client first turns on the system.

c Select the monitor of the Intel® client system to display: **Primary**, **Secondary**, or **Tertiary**.

d Click **Start UCM** to generate a UCM code on the Intel® AMT system, then type the code displayed on the system.

6 Click **Initiate Action** to establish the connection and initiate the required action.

You can't stop a User Consent session while the respective IDE-Redirection session is active.

7 View the policy enforcement status in **Server Task Log**.

8 When you're done with the needed troubleshooting, end the IDE-Redirection connection. See *Stop image redirection*.

Remote systems don't boot until the IDE-Redirection is stopped.

See also

Connect to a system using the Serial-over-LAN on page 109
McAfee KVM Viewer options on page 127

Stop image redirection

You can stop an in-progress image redirection for the selected client systems, as needed.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **System Tree**, select the systems or groups for which IDE-Redirection is active.
2. Click **Actions** | **AMT Actions** | **Stop Image Redirection**, then click **OK**.
3. View the policy enforcement status in **Server Task Log**.
4. Boot or restart the systems normally using the **Normal Boot/Reboot** option, or use SOL to restart the system.

Enforce Intel AMT configuration policy

You can use this action to immediately configure the Intel® AMT capable systems that have a configuration policy assigned to them.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **System Tree**, select the required systems or groups that you want to configure.
2. Click **Actions** | **AMT Actions** | **Enforce AMT Firmware Configuration Policy**, then click **OK**.
3. View the policy enforcement status in **Server Task Log**.
4. Boot or restart the systems normally using the **Normal Boot/Reboot** option, or use SOL to restart the system.

Enforce Intel AMT policies

You can use this action to immediately enforce the Intel® AMT policies of Alarm Clock, Local Access, Remote Access, and KVM, on the selected systems.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **System Tree**, select the required systems or groups where you want to enforce the policies.
2. Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.
3. View the policy enforcement status in **Server Task Log**.

Automate Intel AMT policy enforcement

Create and use the server tasks to enforce Intel® AMT policies and turn on the remote Intel® AMT systems at a scheduled time using out-of-band communication.

If you have many Intel® AMT systems in your network, executing this action on all them at once could have a negative impact on your network by consuming too much bandwidth.

Tasks

- *Schedule and enforce out-of-band AMT policies* on page 112
  You can enforce the existing Intel® AMT out-of-band policy to the Intel® AMT systems at a particular time or at regular intervals.
- *Schedule out-of-band power on* on page 112
  You can choose to turn on your Intel® AMT systems at a particular time or at regular intervals.

Schedule and enforce out-of-band AMT policies

You can enforce the existing Intel® AMT out-of-band policy to the Intel® AMT systems at a particular time or at regular intervals.

Before you begin
Create a query that returns only the fully configured Intel® AMT systems that you want to modify. Make sure that your query returns results in table format. For more information about working with queries, see the McAfee ePO documentation.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, from **Server Tasks**, click **New Task**.
2. In **Description**, type a name for the task that you want to create, a brief description (optional), enable the schedule status, then click **Next**.
3. From **Actions**, select **Run Query** from the drop-down list. From **Query**, click … to select the query you created that returns the configured Intel® AMT systems, then click **OK**.
4. Select a language from the drop-down**Next** list, then in **Sub-Actions**, click …, select **Out-of-Band Enforce AMT Policies**, then click **OK**.
5. Click **Next** and schedule the task as needed.
6. Click **Next** to view a summary of the server task, then click **Save** to return to the **Server Tasks** page.
7. Click **Run** for the corresponding server task that you created.
8. View the task status in **Server Task Log**.

Schedule out-of-band power on

You can choose to turn on your Intel® AMT systems at a particular time or at regular intervals.

Before you begin
Create a query that returns Intel® AMT systems that are configured. Make sure that your query is configured to return the specific subset of systems you want to modify, and that the results are returned in table format. For more information about working with queries, see the McAfee ePO documentation.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, from **Server Tasks**, click **New Task**.

2 In **Description**, type a name for the task that you want to create, a brief description (optional), enable the schedule status, then click **Next**.

3 From **Actions**, select **Run Query** from the drop-down list. From **Query**, click **…** to select the query you created that returns all configured Intel® AMT systems, then click **OK**.

4 Select a language from the drop-down list, then in **Sub-Actions**, click **…**, select **Out-of-Band Power On**, then click **OK**.

5 Click **Next** and schedule the task.

6 Click **Next** to view a summary of the server task, then click **Save** to return to the **Server Tasks** page.

7 Click **Run** for the corresponding server task that you created.

8 View the task status in **Server Task Log**.

Maintenance tasks

You can create independent schedules for each possible configuration, such as reissuance of certificates, renewal of passwords, synchronization of Intel® AMT time, and network settings.

When the maintenance task is executed, these actions are initiated based on the Intel® AMT system configuration:

- **RCS Maintenance** — This action is initiated for Intel® AMT systems in Admin Control mode. Selected maintenance activities are performed.
- **HBC Maintenance** — This action is initiated for Intel® AMT system in Client Control mode. Delta configuration to synchronize all recent changes in the host-based configuration profile is performed, irrespective of the options selected.

The maintenance client task provides these options (applicable only to systems in Admin Control mode):

- **Synchronize AMT Time** — Synchronizes the clock of the Intel® AMT device with the clock of the computer running the Intel® RCS service. This task is performed automatically when any of the other tasks are performed.
- **Synchronize Network Settings** — Synchronizes network settings of the Intel® AMT device based on these:
  - Fully qualified domain name
  - IP address
  - DDNS and DHCP Option 81
- **Re-Issue AMT Certificates** — Reissues the certificates stored in the Intel® AMT device. If the device contains 802.1x certificates, the Intel® AMT administrator password is reset to default.

- **Renew Active Directory Password** — Resets the password of the Active Directory object representing the Intel® AMT system.
- **Renew Administrative Password** — Resets the password of the default Digest admin user in the Intel® AMT device according to the password setting defined in the profile.

Modifying ePO Deep Command settings initiates delta configuration to synchronize data among the server, Intel® RCS system, and Intel® AMT systems.

Tasks

- *Schedule a maintenance task* on page 114
  Create and schedule a maintenance task for the Intel® AMT systems.
- *Compare maintenance tasks* on page 114
  In McAfee ePO 5.0, you can compare two tasks under the same category.

Schedule a maintenance task

Create and schedule a maintenance task for the Intel® AMT systems.

Task

Select these options for systems in Admin Control mode. For Client Control mode systems, delta configuration to synchronize all recent changes in the host-based configuration profile is performed.

Execute this task as per your organization's password and network change policy.

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Policy** | **Client Task Catalog**, then select **AMT Maintenance** under **ePO Deep Command 2.1.0**.
2. Click **New Task**, select **AMT Maintenance** as the task type, then click **OK**.
3. Type a name and description for the task, select the maintenance task to be scheduled, then click **Save**.
4. Click **Assign** in the actions column for the task, select the required system group for which you want to schedule the ePO Deep Command maintenance task, then click **OK**.

   The **Client Task Assignment Builder** wizard appears.
5. In the **Select Task** step, select **ePO Deep Command 2.1.0** as the product, select **AMT Maintenance** as the task type, select the maintenance task, select the inheritance and tag options as needed, then click **Next**.
6. Schedule the task as needed, then click **Next**.
7. Review the summary, then click **Save** to open the **System Tree**.
8. Select the systems or groups where you assigned the task, then click **Actions** | **Agent** | **Wake Up Agents**.
9. Select **Force complete policy and task update**, then click **OK**.

The task is executed on the selected client systems, as scheduled.

Compare maintenance tasks

In McAfee ePO 5.0, you can compare two tasks under the same category.

For detailed information on **Client Task Comparison**, see the McAfee ePO 5.0 product documentation.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Client Task Comparison**, select **ePO Deep Command 2.1.0** as the product, select **AMT Maintenance** as the policy category, then select **Show settings**.

2 Select the tasks to compare in the **Compare Client Tasks** row from the **Policy 1** and the **Policy 2** column lists.

The settings available in the tasks and their values appear for the comparison.

Managing events and logs

Configure events to track configuration changes and any failures reported from Intel® AMT systems, and check issue details in logs.

ePO Deep Command events

When configured to track, these events are logged in the **Threat Event log**.

The ePO Deep Command software generates two kinds of events:

- **Out-of-band events** — Events generated when an Intel® AMT action is triggered on a client system.
- **Configuration events** — Events generated when a configure or unconfigure policy is enforced on Intel® AMT systems.

	Name	ID	Generates when...
Out-of-band events	**Deep Command - Local Fast Call For Help**	34350	A local Intel® AMT system initiates a **Client Initiated Local Access** call for technical help.
	Deep Command - Connected Remote Fast Call For Help	34351	A remote Intel® AMT system initiates a **Client Initiated Remote Access** call.
	Deep Command - Disconnected Remote Fast Call For Help	34352	A remote Intel® AMT system closes a **Client Initiated Remote Access** call.
	Deep Command - Command Not Found	34360	The arbitrary command specified in the policy is not a valid command.
	Deep Command - Command Execution Failed	34361	The arbitrary command specified in the policy fails to execute for some reason. For example, when a user doesn't have sufficient rights to execute the command.
	Deep Command - Maintenance Failure	34367	A maintenance task has failed.
	Deep Command - Maintenance Success	34368	A maintenance task is successfully executed.
	Deep Command - Local User needs help	34369	An event of type CILA_USER is generated when a Local User requests assistance (if the caller identification is enabled).
	Deep Command - Connected Remote Fast Call For Help from User	34371	An event of type CIRA_USER is generated when a connection request for a Remote Fast Call For Help action from the current user is successfully established (if the caller identification is enabled).

	Name	ID	Generates when...
Configuration events	**Deep Command - Configure Failure**	34362	A configuration attempt has failed.
	Deep Command - Unconfigure Failure	34363	An unconfigure attempt has failed.
	Deep Command - Configure Success	34364	A configuration attempt is successful.
	Deep Command - Unconfigure Success	34365	An unconfigure attempt is successful.
	Deep Command - Uncontrolled Unconfigure	34366	An unconfiguration of a system configured by some unknown means is attempted.
	Deep Command - Move to ACM Failure	34373	A migration attempt from Client Control to Admin Control mode has failed.
	Deep Command - Move to ACM Success	34374	A migration attempt from Client Control to Admin Control mode is successful.

Forward events immediately

Configure to forward events with Informational priority immediately to McAfee ePO, which allows the Intel® AMT system to report any failures as they occur.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, navigate to **System Tree**, click the **Assigned Policies** tab, then select **McAfee Agent** from the **Product** menu.
2. Click a policy that you want to modify. For example, click **My Default** under **General** category.
3. In the **Events** tab, select **Enable priority event forwarding**, select **Informational** from the event priority menu, then click **Save**.
4. Enforce the policy using one of these methods:
   - From McAfee ePO, select the systems or groups where you want to assign this policy, then send an agent wake-up call.
   - From the Intel® AMT systems, go to **McAfee Agent Status Monitor** | **Collect and Send Properties** | **Check New Policies** | **Enforce Policies**.

If you don't enforce the policy to the Intel® AMT systems using one of these methods, it is enforced automatically at the next agent-server communication.

Filter events

You can specify which ePO Deep Command events generated from the client systems to forward to the server.

This selection impacts the bandwidth used in your environment, as well as the results of event-based queries.

Events not selected here are never forwarded to the server.

Task

For option definitions, click **?** in the interface.

1. In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**, select **Event Filtering**, then click **Edit** at the bottom of the page.
2. Select **All events to the server** to forward all events, including Intel® client events, to McAfee ePO, or select **Only selected events to the server** and select the Intel® client events that you want to forward.
3. Click **Save**.

The changes are made at the next agent-server communication.

ePO Deep Command logs

See these ePO Deep Command log files on McAfee ePO, Gateway server, Intel® AMT systems, and Intel® RCS systems for details on any issues.

File name	Location	Description
Server logs		
amtservice.log	`..\Program Files\McAfee\<Agent Handler or ePolicy Orchestrator>\DB\Logs\amtservice.log`	Provides a log of Intel® AMT actions, events, and success and failure messages. It is present on the Agent Handler or McAfee ePO system.
AMTGatewayService_out.log	`..\Program Files\McAfee\ePO Deep Command Gateway\logs\AMTGatewayService_out.log`	Provides a log of remote access through the Gateway server. It is present on the system where Gateway server is installed. You can change the debug level of the log file by changing the parameter **Trace Level** in this configuration file: `..\Program Files (x86)\McAfee\ePO Deep Command Gateway\conf\AMTGatewayService_log.config`
Client logs		
AMTCT_out.log	• **For systems running on Microsoft Windows XP and Microsoft Windows Server 2003** — `..\Documents and Settings\Default User\Application Data\McAfee` • **For systems running on other operating systems** — `..\ProgramData\McAfee\ePO Deep Command Client`	Provides the details of client tasks scheduled in an Alarm Clock policy. The information includes the Client Task Execution policy and the message status.
AMTMgmtService_out.log		Provides the status of client tasks executed using Alarm Clock policies.

File name	Location	Description
AMTRCSMgmtService_out.log	`..\Program Files\McAfee \ePO Deep Command RCS Manager\AMTRCSMgmtService _out.log`	Provides a log of RCS Management.
MediationCA_out.log	`..\Program Files\\McAfee \ePO Deep Command RCS Manager\MediationCA_out .log`	Provides a log of RCS plug-in manager.

9 Connecting to Intel AMT systems using KVM

With the McAfee KVM Viewer, you can remotely access Intel® AMT systems using the Keyboard-Video-Mouse (KVM) feature, regardless of the operating system.

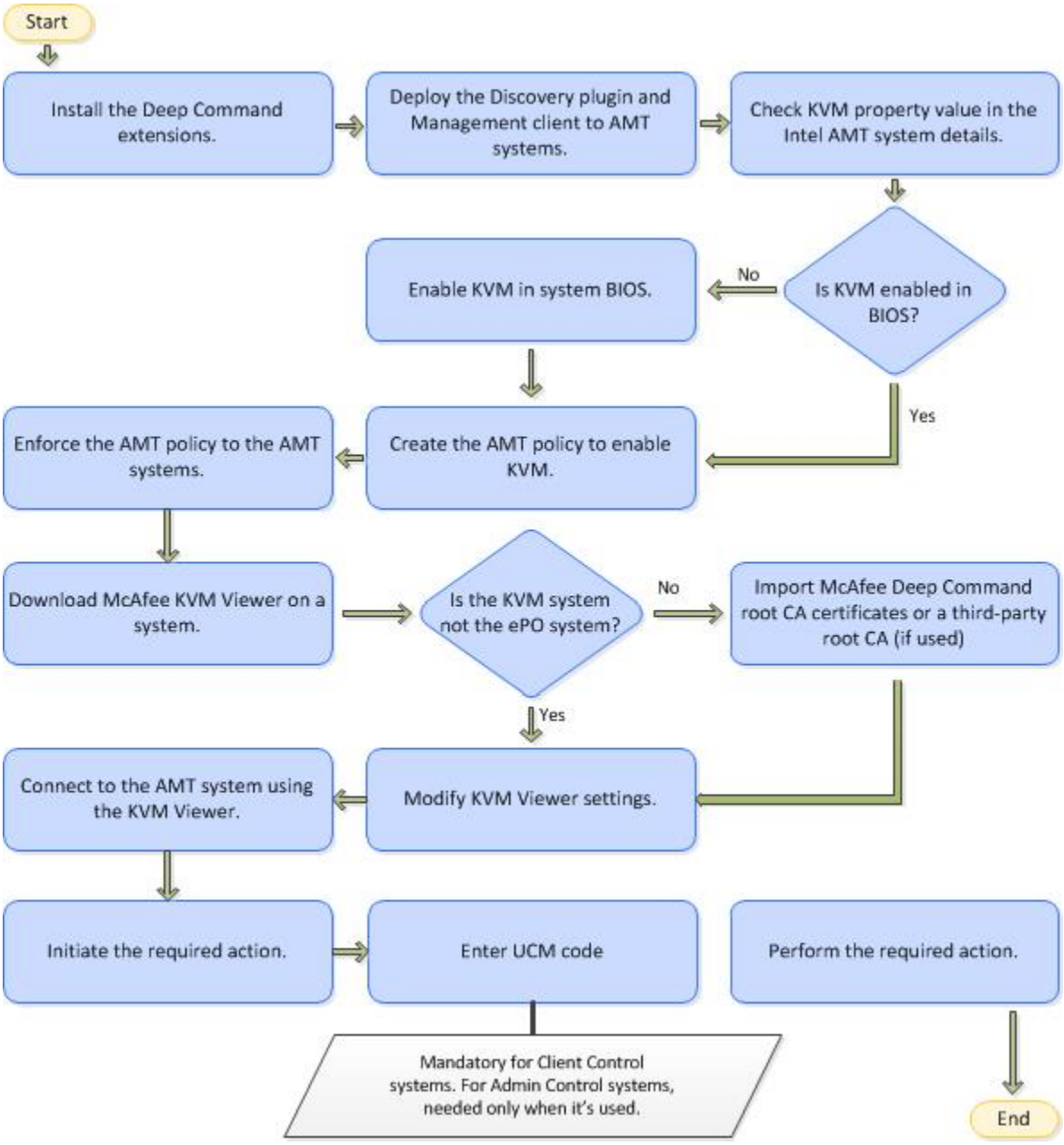
Contents

- *KVM Viewer overview*
- *KVM requirements*
- *Download McAfee KVM Viewer*
- *Set up the client for KVM*
- *Add McAfee root CA certificate*
- *Modify the McAfee KVM Viewer settings*
- *Connect to a local system*
- *Connect to a remote system*
- *Switch the connection to a different system*
- *McAfee KVM Viewer options*

KVM Viewer overview

Use the McAfee KVM Viewer to remotely access your Intel® AMT systems and perform actions such as Power on, shutdown, start or restart them using IDE-Redirection.

Perform these steps to set up your KVM Viewer software and use it for accessing your Intel® AMT systems remotely.


Start
Install the Deep Command extensions.
Deploy the Discovery plugin and Management client to AMT systems.
Check KVM property value in the Intel AMT system details.
Is KVM enabled in BIOS?
No
Enable KVM in system BIOS.
Yes
Create the AMT policy to enable KVM.
Enforce the AMT policy to the AMT systems.
Download McAfee KVM Viewer on a system.
Is the KVM system not the ePO system?
No
Import McAfee Deep Command root CA certificates or a third-party root CA (if used)
Yes
Modify KVM Viewer settings.
Connect to the AMT system using the KVM Viewer.
Initiate the required action.
Enter UCM code
Mandatory for Client Control systems. For Admin Control systems, needed only when it's used.
Perform the required action.
End

KVM requirements

Make sure that your system meets these requirements to connect to a system from McAfee KVM Viewer.

System	Requirements
KVM host system (from where the McAfee KVM Viewer connection is initiated)	If using a Windows XP or Windows Server 2003 system, it must have: • Windows Remote Management (WinRM) • Microsoft .NET Framework 3.5 SP1
KVM target client system (An Intel® AMT system)	• **Version**: 6.0 or later • **Graphics**: Intel® integrated 3000 or higher

Download McAfee KVM Viewer

Download McAfee KVM Viewer from **Software Manager**, then save it to a system from where you want to access your Intel® AMT systems.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.

2 On the **Software Manager** page under **Product Categories**, click **Software Not Checked In** | **Licensed**.

3 Select **McAfee ePO Deep Command 2.1** from the products list, click **Download** next to **McAfee KVM Viewer**, then save the .zip file.

4 Extract the .zip file to obtain the **MKVMView.exe** file to access the McAfee KVM Viewer.

Set up the client for KVM

Configure the KVM policy, then enforce it to the Intel® AMT systems.

Before you begin

Create a KVM policy to enable KVM.

Task

For option definitions, click **?** in the interface.

1 In the **System Tree**, select the systems that you want to access remotely.

2 Click **Actions** | **AMT Actions** | **Enforce AMT Policies**, then click **OK**.

See also

Create a KVM policy on page 100

Add McAfee root CA certificate

Import the McAfee ePO Deep Command root CA certificate to the KVM host system to authenticate a KVM connection. This task is required only when the KVM host system is not the same system where McAfee ePO is installed.

Before you begin

Export the McAfee ePO Deep Command root CA certificate from McAfee ePO. See *Export an active certificate* for instructions.

Import the certificate file using one of these methods.

Tasks

- *Place the certificate manually* on page 122
  Place the McAfee ePO Deep Command root CA certificate file to the KVM directory.
- *Import the certificate in KVM console* on page 122
  You can import the certificate in the McAfee KVM Viewer console.
- *Use Microsoft Management Console* on page 123
  Add the McAfee ePO Deep Command Root CA certificates, when used, to the certificate store of the system where you're accessing the McAfee KVM Viewer for the connection.

See also

Modify the McAfee KVM Viewer settings on page 123
Export an active certificate on page 30

Place the certificate manually

Place the McAfee ePO Deep Command root CA certificate file to the KVM directory.

Task

For option definitions, click **?** in the interface.

1 Rename the McAfee ePO Deep Command root CA certificate file to `DefaultCA.crt`.

2 Copy the renamed file and place it in the McAfee KVM Viewer directory.

Import the certificate in KVM console

You can import the certificate in the McAfee KVM Viewer console.

Task

For option definitions, click **?** in the interface.

1 From the KVM host system, browse to the folder where McAfee KVM Viewer is stored, then double-click the **MKVMView** file.

2 On the **McAfee KVM Viewer Connection** page, click **Options** to view the settings.

3 In the **General** tab, complete the settings as required to establish the connection.

See *Modify the McAfee KVM Viewer settings* for instructions.

4 In the **Advanced** step, click **Import** under **TLS Certificates**, then browse to select the trusted root certificate.

5 Click **Yes** on the **Security Warning** screen, then click **Apply** to save the settings.

Use Microsoft Management Console

Add the McAfee ePO Deep Command Root CA certificates, when used, to the certificate store of the system where you're accessing the McAfee KVM Viewer for the connection.

Before you begin

Export the McAfee ePO Deep Command Root CA from **Server Settings** | **Intel AMT credentials** | **Edit** page. See *Export an active certificate* for instructions.

Task

1. In the KVM host system, run `mmc` from the command prompt.
2. From **File**, click **Add/Remove Snap-in**, select **Certificates**, then click **Add**.
3. From the **Certificates snap-in** window, select **My user account**, click **Finish**, then click **OK**.
4. In **Console Root**, expand **Certificates - Current User** | **Trusted Root Certification Authorities**, right-click **Certificates**, then click **All Tasks** | **Import**.
5. In the Certificate Import wizard, click **Next**, then browse to and select the McAfee ePO Deep Command Root CA certificate (for example, `CN_McAfee_ePO_Deep_Command_Root_2013-04-17_01_53_04.crt`), click **Next**, click **Next** again, then click **Finish**. If you receive a security warning, click **Yes**, then click **OK** to confirm.

See also

Export an active certificate on page 30

Modify the McAfee KVM Viewer settings

Provide settings required for a successful connection.

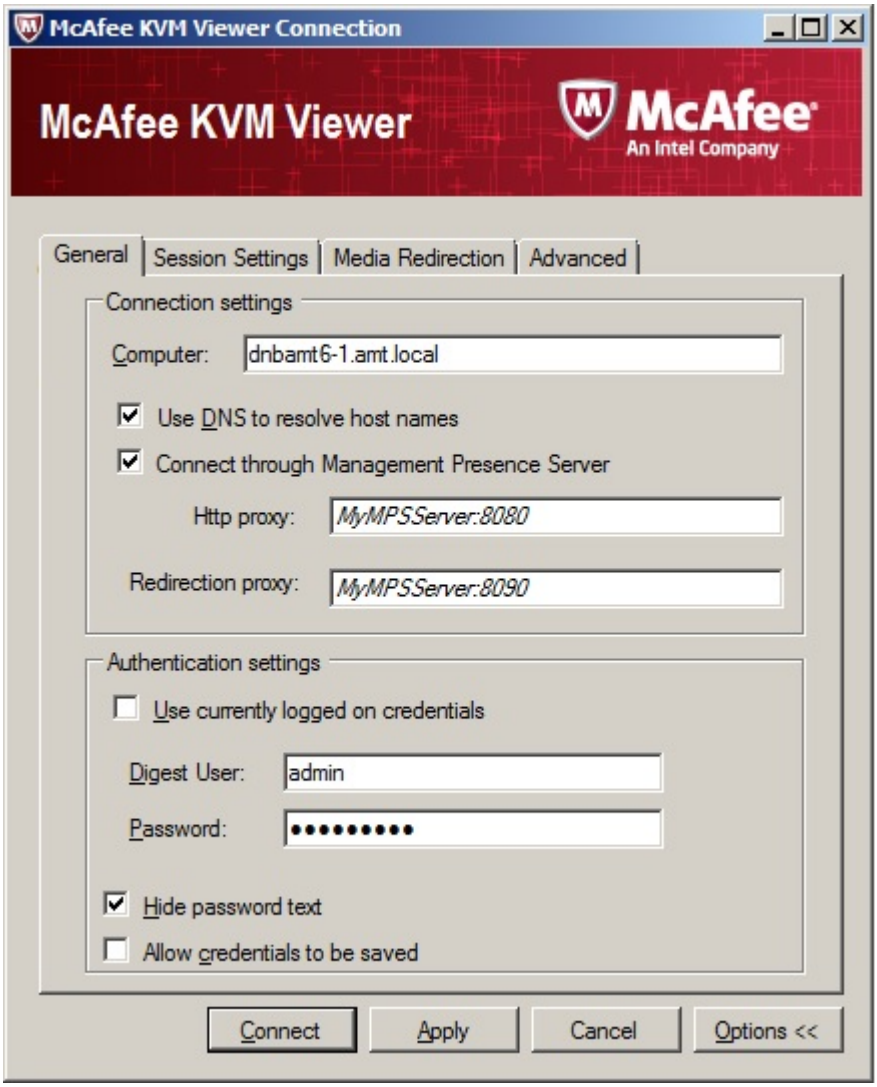
Before you begin

Make sure that the required certificates are available in the certificate store of the KVM system. For information on adding the ePO Deep Command Root CA certificate, see *Add a McAfee ePO Deep Command Root CA certificate*.

Task

1 From the KVM host system, browse to the folder where McAfee KVM Viewer is stored, then double-click the **MKVMView** file.

2 On the **McAfee KVM Viewer Connection** page, click **Options** to view the settings.



3 In the **General** tab, complete these settings:

- **Computer** — Type the host name of the managed client.
- **Use DNS to resolve host names** — Resolve any NetBIOS name or IP address to its FQDN (fully qualified domain name).
- **Connect through Management Presence Server** — Make a connection through the Gateway server. Provide the FQDN of the Agent Handler where the Gateway server is installed, and the port numbers for HTTP proxy and Redirection proxy (SOCKSv5). Use the format `<Gateway_server>:<port_number>`.

  This option is required only for Remote Access.

- **Authentication settings** — Provide credentials used in the configuration profile policy or under Intel® AMT credentials in **Server Settings**. Or select **Use currently logged on credentials** if the logon user has the required permission in the configuration profile.
  - **Digest User** — The Intel® AMT digest user name for the managed client (displayed only when **Use currently logon credentials** is not selected).
  - **Password** — The Intel® AMT digest user password for the managed client (displayed only when **Use currently logon credentials** is not selected).
  - **Hide password text** — Hide the text entered in the **Password** field (displayed only when **Use currently logon credentials** is not selected).
  - **Allow credentials to be saved** — Store the user name and password for use in subsequent sessions (displayed only when **Use currently logon credentials** is not selected).

4 (Optional) In the **Sessions Settings** tab, select the monitor to display if the client has more than one monitor.

Configure the default monitor preference in the KVM policy. Don't change the preference in the McAfee KVM Viewer settings.

5 (Optional) In the **Media Redirection** tab, browse to and select the image file (.ISO) to use for media redirection operations.

6 In the **Advanced** step, complete these steps:

- **Logging** — Select the logging level to store the Intel® AMT log files: **Normal** or **Verbose**.
- **TLS Certificates** — Click **Import**, then browse to and select the trusted root certificates that are required to verify McAfee KVM Viewer sessions.
- **Wireless retry settings** — (Optional) Select **Automatically attempt to reestablish lost wireless connections**, then select the number of retries and their interval (in seconds).

  This option is required only when connecting to a system over a wireless connection.

7 Click **Apply** to save the settings.

See also

Add McAfee root CA certificate on page 122

Connect to a local system

Connect to a local Intel® AMT system to send power control commands to the client.

Task

1 From the KVM host system, browse to the folder where the McAfee KVM Viewer is stored, then double-click the **MKVMView** file.

2 In the **Computer** field, type the IP address, FQDN, or NetBIOS name of a managed client.

From the drop-down menu, you can select a client that was connected previously.

3 Click **Connect** to establish the connection.

If prompted to enter a client consent code, obtain the consent code from the user of the client system, then enter the code to connect.

If the client system was configured using the host-based configuration, the user consent is required.

The connection status is displayed when connecting.

On successful connection, the KVM Viewer window displays the client screen.

Connect to a remote system

Connect to a remote Intel® AMT system to send power control commands to the client.

Task

For option definitions, click **?** in the interface.

1 From the KVM host system, browse to the folder where the McAfee KVM Viewer is stored, then double-click the **MKVMView** file.

2 Click **Options** to open the KVM setting options.

3 In the **Computer** field, type the IP address, FQDN, or NetBIOS name of a managed client.

From the drop-down menu, you can select a client that was connected previously.

4 Select **Connect through Management Presence Server**, then type HTTP proxy and Redirection proxy (SOCKSv5) in the format `<MPS_Proxy_server>:<port_number>`.

5 Click **Connect** to establish the connection.

If prompted to enter a client consent code, obtain the consent code from the user of the client system, then enter the code to connect.

If the system was configured using the host-based configuration, the user consent is required.

The connection status is displayed when connecting. When connecting to a wireless client, an entry for each retry event is displayed.

On successful connection, the KVM Viewer window displays the client screen.

Switch the connection to a different system

You can switch KVM connection from one Intel® AMT system to the other.

Task

For option definitions, click **?** in the interface.

1 From the McAfee KVM Viewer screen, click **Connection** | **Stop**.

The current active session is stopped.

2 Click **Tools** | **Options**, from the **General** tab, specify the needed Intel® AMT system in the **Computer** field, then click **Connect**.

The connection is switched to the selected Intel® AMT system.

You can connect to multiple Intel® AMT systems from the same KVM host system by starting multiple instances of McAfee KVM Viewer and connecting to a different system in each instance.

McAfee KVM Viewer options

Once you connect to a client system, use the menu bar options in the KVM console to perform required actions.

Option	Suboption	Description
File	**Exit**	Closes the **McAfee KVM Viewer** page. An active IDE-Redirection session does not end when the McAfee KVM Viewer is closed.
Connection	**Start**	Starts a connection to the client system.
	Stop	Ends a connection to the client system.
	Refresh	Reloads the screen in display.
	Color Quality	Allows selecting the quality of the video component: **Maximum**, **Medium**, or **Low**.
	Scale Video	Allows resizing the screen to a specific percentage.
	Full Screen	Displays the screen in Full Screen mode.
Tools	**Send Ctrl-Alt-Del**	Sends `Ctrl-Alt-Del` command to the client system.
	Power Control	Sends the Intel® AMT power control commands to the client system: • **Power Up** — Select to power up your Intel® AMT system. • **Power Down**— Select to shut down your Intel® AMT system. • **Power Reset** — Select to restart your Intel® AMT system. • **Boot with IDER** — Select to boot the Intel® AMT system from using IDE-Redirection device. This device must be configured on the **Media Redirection** tab. • **End IDER Session** — Select to end the IDE-Redirection session (available only when an IDE-Redirection session is active).

Option	Suboption	Description
	Wireless Link Preference	Allows selecting the link preference for a session connected over a wireless connection. For a system that has Intel® AMT version earlier than version 8.1, select **Management Engine** preference. This allows restarting the system using an Intel® AMT action such as IDE-Redirection.
Help	**About McAfee KVM Viewer**	Displays the version and copyright information of the McAfee KVM Viewer.

10 Troubleshooting

Error messages are displayed by programs when an unexpected condition occurs that can't be fixed by the program itself. Use this list to find an error message, an explanation of the condition, and any action you can take to correct it.

Remote configuration

You might see these errors while setting up an Intel® AMT configured using remote configuration.

When configuring Intel® Active Management Technology (AMT) using the ePO Deep Command AMT Configuration policy, an exit code is logged in **Threat Event Log** and ACUConfig.log. Here are the issues with a brief explanation on how to interpret and address these issues.

Issue	Description	Corrective action
Exit code 0	The requested operation completed successfully	None
Exit code 3	Occurs when one of these conditions is true: • This system does not have Intel® AMT hardware. • Intel® AMT firmware is disabled in the Intel® MEBX. • Required drivers are not installed or enabled.	Validate the ePO Deep Command Discovery and Reporting data. If the platform supports Intel® AMT, use the SystemDiscovery command. For more information, see https://planet.mcafee.com/docs/DOC-8930.
Exit code 4	This system supports Intel® Small Business Advantage (Intel® SBA). The Intel® SBA systems are designed for small businesses. They can only be configured using the software included with Intel SBA, and not using Intel® RCS.	Unsupported platform. Remove such systems from the Intel® AMT configuration policy.
Exit code 6	The Intel® RCS failed to process the request.	Validate whether the Intel® RCS server is operational and correctly configured. For information on Intel® RCS installation and configuration, see https://community.mcafee.com/docs/DOC-4292.
Exit code 7	The Intel® AMT device does not have a PSK, which is a prerequisite for the requested operation.	This issue occurs only when the Pre-Shared Key Alternative Configuration is used. For information on how to insert a valid PSK into the firmware, see https://community.mcafee.com/docs/DOC-4211.

Issue	Description	Corrective action
Exit code 32	A certificate request has been sent to the Certification Authority but the created certificate has put it into "Pending Requests" or "waiting for approval". Intel® SCS does not support pending requests.	Request Handling of the Microsoft CA must allow automatic issuing of the certificate per setting provided. For instructions to enable automatically issuance of certificates, see https://community.mcafee.com/docs/DOC-4214 for standalone CA or see https://community.mcafee.com/docs/DOC-3314 for enterprise CA.
Exit code 33	Failed to request the certificate.	Make sure that the Microsoft CA is operational. For instruction on how to configure it, see https://community.mcafee.com/docs/DOC-4214 for standalone CA or see https://community.mcafee.com/docs/DOC-3314 for enterprise CA.
Exit code 38	The certificate cannot be retrieved because access to the Certificate Authority is denied.	Make sure that appropriate permissions defined for Intel® RCS server to Microsoft CA. For instructions on how to grant permissions to the Intel® RCS users, see https://community.mcafee.com/docs/DOC-4214 for standalone CA or see https://community.mcafee.com/docs/DOC-3314 for enterprise CA.
Exit code 45	TLS cannot be configured because cryptography is disabled on this system.	Platform is not compatible for use with ePO Deep Command. The **Hardware Crypto Enabled** property in the **Deep Command** tab on the system properties page must be enabled. OEM determines this setting during the system manufacturing process and it cannot be changed afterward.
Exit code 75	Failed to complete remote configuration of this Intel® AMT device.	Validate the WMI\DCOM permissions and remote configuration certificate settings. For information on Intel® RCS installation and configuration, see https://community.mcafee.com/docs/DOC-4292.
Exit code 78 (AMT status: Not ready when I try to configure a client)	This issue might occur when the client is Intel® AMT-equipped but AMT is disabled in BIOS. The device manufacturer might not have configured Intel® AMT capabilities on this system.	Contact your administrator or device manufacturer's support for the solution.
Exit code 80	The Intel® Management Engine Interface (MEI) driver is not installed or cannot be accessed.	Preliminary report of systems affected is displayed using dashboards based on ePO Deep Command Discovery & Reporting data. Intel® MEI driver can be obtained from the OEM support drivers download.

Issue	Description	Corrective action
Configuration/ unconfiguration task fails with this error in **Server Task Log**: Intel® AMT unconfiguration failed. Initial connection to the Intel® AMT device failed. A TCP error occurred. Make sure that the destination settings are correct and that a network connection exists to the target.	This error occurs when the Intel® AMT systems cannot resolve FQDN of the Intel® RCS server or conversely.	Make sure that the DNS settings for the Intel® AMT system or Intel® RCS server are not configured to use both IPv4 and IPv6.
Configuration attempt to a system outside the domain fails.	If a configured Intel® AMT system is outside the home domain, it cannot be unconfigured from McAfee ePO.	Unconfigure the client system manually.
Server task log displays a configuration policy enforcement status as "completed" when it actually fails.	ACUConfig has an issue where it might set operating system return code to "0:Success", when it actually experienced a failure. McAfee ePO determines the policy enforcement status based on this return code.	View the correct status by navigating to **Server Task Log** | **Configure AMT Firmware** | **Subtask** | **<target machine>**.

Host-based configuration

You might see these errors while configuring an Intel® AMT system configured using host-based configuration.

Issue	Description	Corrective action
Configuration task fails without an error	This issue might occur if the firmware or MEI driver version is not compatible.	Update the Intel® AMT firmware and Intel® MEI driver. Contact your hardware vendor to obtain the latest drivers.
Configuration task fails with this error: Error in notifying listeners of message Type HOSTBASED_CONFIGREQUEST	This issue might occur when the Intel® AMT properties are not updated after a recent reinstallation of ePO Deep Command extensions.	Send an agent wake-up call with **Get full product properties**.

Intel® AMT actions

You might see these errors while enforcing Intel® AMT actions to your client systems.

Issue	Description	Corrective action
HTTP 401 in AMTservice.log	This issue occurs when the server is not able to authenticate and connect to the Intel® AMT system.	Verify that the user name and password are correct on the **Edit Intel® AMT Credentials** page.
Openwsman last error = 12029 in AMTservice.log	This error can occur if the TCP Port 16993 on the Intel® AMT system is not accessible from McAfee ePO.	See *Required ports* and verify that the required firewall ports are allowed on the Intel® AMT system and on McAfee ePO.
Openwsman last error = 12002 in AMTservice.log	This error occurs if the Intel® AMT system is not reachable and the request times out.	None
Openwsman last error = 12175 in AMTservice.log	This issue might occur when McAfee ePO is in a different domain than the Intel® AMT systems.	Verify these settings: • The Intel® AMT system nodes are configured using intermediate CA certificates. • The certification of the CA is getting resolved from McAfee ePO. • The system account of McAfee ePO does have the required trusted CA to perform Intel® AMT actions.
Failed to test the connection to the Intel®) AMT device after configuration completed in ACUConfig.log or in **Server Task Log** (if initiated using Intel® AMT action)	This error appears in the log when a Windows Server 2003-based or Windows XP-based client system cannot obtain certificates from a Windows Server 2008-based certification authority (CA) server, which uses SHA2 256 encryption or higher encryption (SHA2 384 or SHA2 512).	Install hotfixes mentioned in these Microsoft articles to resolve this issue: • Microsoft KnowledgeBase article # 968730 (http://support.microsoft.com/kb/968730) • Microsoft KnowledgeBase article # 938397 (http://support.microsoft.com/kb/938397
The **Enforce AMT Firmware Configuration Policy** option is disabled for some Intel® AMT systems.	This issue might occur when the Intel® AMT firmware version is reported from the clients.	Update the Intel® AMT firmware and Intel® MEI driver. Contact your hardware vendor to obtain the latest drivers.
Normal boot or restart fails	Intel® AMT credentials are incorrect — `amtservice.log` displays HTTP 401 error	Make sure that the correct credentials and certificates are uploaded in **Server Settings** on the **Edit Intel® AMT Credentials** page.
	Domain name and FQDN of the Intel® AMT system are not resolvable from McAfee ePO.	Verify that the domain and FQDN of the Intel® AMT system is correctly resolved from McAfee ePO.
	The required ports are blocked.	Verify that the required Firewall Ports are allowed on the Intel® AMT system and McAfee ePO.

Serial-over-LAN

Issue	Description	Corrective action
SOL connection to an Intel® AMT system fails with errors in SOL terminal	**Authentication Failure** — Invalid credentials.	Provide the correct credentials in **Server Settings** | **Intel® AMT Credentials**.
	Busy — An SOL connection to the Intel® AMT system is already established.	Only one SOL connection at a time is allowed.

Issue	Description	Corrective action
	Socket Error — Redirection port is not enabled on the Intel® AMT System. This error also occurs when a certificate or authentication fails.	Enforce an AMT Policy to enable the Redirection Port and try again. Make sure that a valid certificate and credentials are used.
	Maximum Connections Reached — Maximum SOL connections that are allowed by Agent Handler has been made.	Agent Handler allows only four active SOL sessions at a time. Disconnect one of the SOL sessions and try again.
	If the issues persists, perform these steps: • Verify that the required firewall ports are allowed on the Intel® AMT system and McAfee ePO. • Confirm that the Intel® AMT system domain and FQDN is correctly resolved from McAfee ePO. • Wait three seconds before trying to connect or disconnect the SOL session.	
BIOS can't be redirected to the SOL terminal	Credentials are incorrect	Make sure that the correct credentials are provided in **Server Settings** | **Intel® AMT Credentials**.
	The required ports are blocked.	Verify that the required firewall ports are allowed on the Intel® AMT system and McAfee ePO.
SOL connection through a local Agent Handler is failing.	This issue occurs when Intel® AMT system is not accessible from the Agent Handler.	Perform these actions to resolve the issue: • If the Intel® AMT system is moved from one Agent Handler to another and SOL connection is tried before the agent-server communication to update this change, wait for the next agent-server communication. • Make sure that the port 16995 is not blocked in the firewall. • Assign the local Agent Handler to the target system from **Menu** | **Configuration** | **Agent Handlers** | **New Assignment**. See the McAfee ePO documentation for detailed instructions.

IDE-Redirection

Issue	Description	Corrective action
IDE-Redirection session does not initiates	This issue might occur due to various reasons.	Perform these checks, then perform the corrective action based on the error in `amtservice.log`: • Make sure that IDE-Redirection (IDE-R) is supported and enabled on the **System Properties Intel® AMT** page. • Verify that the correct credentials and certificates are uploaded in the Server Settings **Intel® AMT Credentials** page. • Make sure that the system is not in an active IDE-R session before initiating the IDE-R session.
	Authentication Failure or HTTP 401 error or IDE-R Session Closed — Invalid credentials.	Verify that the correct user name and password are provided in **Server Settings | Intel® AMT Credentials**.
	TLS Connection Failure — certificates not imported.	Verify that the certificates imported in **Server Settings | Intel® AMT Credentials**
	Invalid Parameter — ISO not found.	Verify that the shared ISO image path is correct and it is accessible by the Agent Handler.
	Socket Error — The system is not reachable from Agent Handler.	Verify that the system is properly connected and the system is reachable the Agent Handler.
	Maximum Connections — Four IDE-R sessions are already active through the Agent Handler.	Stop one of the active IDE-R sessions and then try again.
	If the issues persists, perform these steps: 1 Verify that the required Firewall Ports are allowed on the Intel® AMT system and on McAfee ePO. 2 Verify that the domain of the Intel® AMT system is being correctly resolved from McAfee ePO. 3 Confirm that the FQDN of the Intel® AMT system is correctly resolving from McAfee ePO. 4 Verify that the domain of the shared folder is correctly resolving from the Agent Handler and the shared file is accessible.	
IDE-Redirection is not working in Local Access environment.	It might be due to the Universal Naming Convention (UNC) share is not accessible from ServiceAMT because of the domain authentication policy for UNC share.	Make sure that — • The recovery operating system image file is an .iso file shared on a UNC mount. • The UNC share is accessible by the Agent Handler and using the system account. • The path has been defined using the UNC syntax rather than using the IP address.

Remote Access using the Gateway server

Issue	Description	Corrective action
Remote Access connection fails with "Unknown CA" error in the Stunnel log	This might occur if the root CA certificate is not imported into the Management Engine Certificate Store of the Intel® AMT systems.	Make sure that the required certificate is added successfully.
Remote Access connection fails with a "certificate unknown" error in the Stunnel log	This issue occurs when the Stunnel configuration and management certificates are not in sync.	1 In the Intel® Commander, check whether the CA is present in Intel® Management Engine Certificate Store. 2 In the Stunnel configuration, check whether the CA in Stunnel and certificate store are the same.

McAfee KVM Viewer

Issue	Description	Corrective action
McAfee KVM Viewer fails without an error.	None	Make sure that these requirements are met: • Intel® AMT system is accessible from the KVM server. • Credentials provided are correct. • Root Certificate is selected in the KVM certificate.
Remote Access to Intel® AMT system from McAfee KVM Viewer fails.	Auto proxy settings in the McAfee KVM Viewer are not configured.	From **Advanced** tab in **McAfee KVM Viewer**, click **Remote Access**, then configure these settings in the **MPS Auto Proxy Configuration** page.
	The validity of auto proxy list expires. By default, the Intel® AMT systems added to the Auto proxy list can be connected again within 8 hours.	Navigate to **McAfee KVM Viewer** | **Advanced** | **MPS Auto Proxy Configuration**, delete the Intel® AMT system entry from Auto proxy list, then add it again.
	In VM environment, this issue might happen due to low availability of resources.	Free up memory space on the system and try again.
McAfee KVM Viewer fails with "authentication failed" error in the KVM Viewer log and "Disconnected" in the KVM Viewer status.	This issue might occur when you're using Kerberos credentials while in the configuration profile, Digest authentication is selected.	Access the Intel® RCS console and check the profile configuration. If **Digest User** is selected for **User Type** in the profile, provide the Digest logon credentials in McAfee KVM Viewer. In McAfee KVM Viewer, click the **General** tab, click **Options**, deselect **Use currently logged on credentials**, then enter the Digest user name and password.
While connecting a McAfee EEPC client from McAfee KVM Viewer, cursor behaves abnormally on the Pre-boot authentication screen.	This occurs when the cursor is kept idle for more than 5 minutes.	Press **Tab** to move cursor to the next field.

Wireless

Issue	Description	Corrective action
IDE-Redirection over a wireless connection fails with this error: Boot disk missing, please insert boot disk and press ENTER	Wireless link can't be established because of some network issues.	Fix the connectivity issues in your network, then retry the IDE-Redirection from McAfee ePO or KVM server.
	No wireless Admin or User profile is created on the Intel® AMT system.	Create at least one wireless Admin or User profile on the system.
	The image is not located in the provided UNC path.	Create a UNC share repository, then provide it's read-only permission to all required users in your network.
McAfee ePO can't communicate to an Intel® AMT system where an out-of-band action is performed over a wireless connection. The AMTService.log displays error 12002, 12007, or 12029.	12002 — Intel® AMT system IP address has changed and it's not updated.	Make sure that the DNS configuration is updated every time the system IP address changes.
	12007 — No wireless Admin or User profile is created on the Intel® AMT system.	Make sure that a valid wireless Admin or User profile is created on the system.
	12029 — Required drivers are missing.	Make sure that the required drivers such as Intel® PROSet or Intel® LMS drivers are present, and other requirements are met on the Intel® system.

General issues

Issue	Description	Corrective action
If an Intel® AMT system is in sleep state, it does not respond to User Consent Mode. A related error is logged in AMTservice.log.	None	Change the system power state to *Working*, then try the steps again.
Event filtering does not work on CILA and CIRA events	Event filtering is designed for McAfee Agent generated events. CILA events are generated from Intel® AMT systems, henceforth these events cannot be filtered.	Navigate to **Menu** | **Configuration** | **Server Settings** | **Event Filtering**, select **Only selected events to the server**, then remove **Deep Command** events that are not required.
Intel® AMT policy enforcement fails with this error in AMTservice.log: Unable to determine timezone of Intel® ME. Clocks out of sync (more than +/- 15 minutes)	This issue occurs when you use Active Directory integration and the system time of Intel® AMT system and domain controller are not synchronized (difference more than plus or minus 15 minutes).	None

Issue	Description	Corrective action
Intel® AMT policy enforcement fails with errors similar to these errors in AMTservice.log: • Failed to convert time of Intel® ME • Failed to convert current time • Failed to convert alarm time	This issue occurs when the system call cannot obtain current time of the Intel® AMT system.	None
CILA/CIRA access calls fail with this error in AMTservice.log: Unknown action type (<Action>)	This issue occurs when the required plug-ins are not registered to process CIRA/CILA calls.	None
Boot/reboot with options on a client fails with this error in AMTservice.log: Failed to set the AMT power state	This issue occurs when the Boot/Reboot with options feature is disabled in BIOS.	None
Intel® AMT policy enforcement on a client fails with this error in AMT service.log:Failed to enable redirection, SOL and IDE-R might not work correctly: <Exception Message>	This issue occurs when the Intel® AMT system is not configured.	None
Intel® AMT policy enforcement on a client fails with this error in AMTservice.log: Failed to get OptIn policy: <Exception Message>	This issue occurs when the Intel® AMT version on the client is less than 6.2.	None
Intel® AMT policy enforcement on a client fails with this error in AMTservice.log: Failed to set KVM Settings: <Exception Message>	This issue occurs when KVM feature is not supported on the Intel® AMT system such as on Intel® AMT versions below 7.0.	None
Intel® AMT policy enforcement on a client fails with errors similar to these errors in AMTservice.log: • Failed to set Alarm Clock: <Exception Message> • Failed to disable Alarm Clock	This issue occurs when Alarm Clock feature is not supported on the Intel® AMT system such as on Intel® AMT versions below 5.0.	None
Intel® AMT policy enforcement on a client fails with this error in AMTservice.log: Failed to get system timezone bias	This issue occurs when the client has not collected time zone property of the Intel® AMT system.	None
Intel® AMT policy enforcement on a client fails with this error in AMTservice.log: Failed to get alarm time from policy	This issue might occur when the policy settings are not correct.	None

Issue	Description	Corrective action
Remote Access request using **Get Technical Help** in the Intel® Management and Security Status tool fails with an error stating that the organization is not reachable.	None	1 From the Intel® AMT system, open Mozilla Firefox and access your DMZ Agent Handler system where ePO Deep Command Gateway Server is running. The URL must include the port where Stunnel is running. Firefox shows an SSL certificate warning in your browser. If using Internet Explorer, you might have issues viewing the certificates. 2 View the SSL certificate and verify that it has been issued to the host name of the ePO Deep Command Gateway Server, which is resolvable from the Internet. 3 Verify that the issuer of the certificate is the same CA that has been used for configuring the Intel® AMT system or is known to the Intel® AMT system. 4 Make sure that the ePO Deep Command Gateway Server Logs (`AMTGatewayService_out.log`) and the `amtservice.log` are in the Agent Handler system. 5 Make sure that the DNS resolution is working properly on the ePO Deep Command Gateway Server and unnecessary services are not running on the system. Disable any services like IP address Helper or Ipv6 Services if they are not in use and try again.
Management Framework extension check-in fails	This issue might occur when the Discovery and Reporting extension is not installed.	Install the Discovery and Reporting extension before installing the Management Framework extension.
Intel® AMT properties shown as Not Available after reinstalling the ePO Deep Command extension and executing agent-server communication on the Intel® AMT system	This issue occur when the Intel® AMT properties have not been retrieved from the system. The agent sends only the incremental properties because there have been no changes between detections.	Send an agent wake-up call with **Get full product properties**.
ePO Deep Command dashboard remains after removing its extensions	This issue occurs only with McAfee ePO version 4.6.x.	Select the dashboard, then select **Delete** from the **Dashboard Actions** to delete it manually.

Issue	Description	Corrective action
Alarm Clock policy doesn't enforce	This issue might occur due to various reasons.	Perform these checks, then perform the corrective action based on the error in `amtservice.log`: • Make sure that the Intel® AMT system is in the Post-Configured state and the **System Properties Intel® AMT** page is updated. • Confirm that the AMT tag is applied to the system in **System Tree** and the Alarm Clock policy is saved correctly.
	Authentication Failure or **HTTP 401 error**	Verify that the correct user name and password are provided in **Server Settings** | **Intel® AMT Credentials**
	Failed to create alarm clock service	• Make sure that the system supports the Intel® AMT Alarm Clock feature. • From the client system Intel® ME, the time must be set to UTC if Kerberos is used for authentication. • Verify that the client system Intel® ME time and Agent Handler time are in sync (plus or minus 15 minutes). • Verify that the required Firewall Ports are allowed on the Intel® AMT system and on McAfee ePO. See *Required ports* for the list of ports required for this operation.

Alarm Clock Policy fail to set the time saved in the policy	There's a conflict with the Intel® ME time.	Set the Alarm Clock Time policy for at least five minutes ahead of Intel® ME. Also, consider these:
		• If the Alarm Clock settings are not ahead of Intel® ME time:
		  • When a repeat interval is set, the Alarm Clock is adjusted to the execution time.
		  • When no interval is set, the Alarm Clock is adjusted to 24 hours.
		• If randomization is enabled, a random time is added.
		• If in doubt, set the Agent Handler log level to eight. The times and dates used for calculating the Alarm Clock are displayed.

Issue	Description	Corrective action
Some AMT commands not work when selected from **Automatic Response** | **New Response** | **Actions** | **Run System Command**	Some of the McAfee ePO commands are targeted for troubleshooting purposes and also require manual inputs from the user.	You can use these automatic Response action • **Out-of-Band Enforce AMT Policies** • **Out-of-Band Power On**
ePO Deep Command policies enforcement and actions fail after an upgrade to McAfee ePO 4.6	This issue might occur when there are orphaned branch nodes in the McAfee ePO database.	Run the following SQL script to remove the orphaned branch nodes: `Delete from EPOBranchNode where ParentID NOT IN (Select AutoID from EPOBranchNode) and Type = 3` You might need to run this SQL command multiple times until SQL returns `0 row(s) affected`.

11 Frequently asked questions

Here are answers to frequently asked questions.

Power on and Normal boot or restart

What happens if a normal boot or restart is executed on a system that is in Hibernate or Standby mode?

The system is restored to a normal running state.

Is a user on an Intel® AMT system notified if a normal start or restart is initiated from McAfee ePO?

No, the user is not notified and the system restarts immediately.

What is the amtservice.log file and where is it located? How do you increase the debug level for this log file?

The `amtservice.log` file is present on the Agent Handler system where Intel® AMT actions, events, and success and failure messages are logged.

On a 64-bit McAfee ePO system, the location is `C:\Program Files (x86)\McAfee\ePolicyOrchestrator\DB\Logs`.

On a 32-bit McAfee ePO system, the location is `C:\Program Files\McAfee\ePolicyOrchestrator\DB\Logs`.

To increase the debug log level, go to the **Registry Editor** | **HKEY_LOCAL_MACHINE** | **Network Associates** | **ePolicy Orchestrator** | **Log Level**, and change the value to 8.

What do I do if a normal boot or restart for an Intel® AMT system fails?

1. Make sure that the correct credentials and certificates are uploaded in **Server Settings** on the **Edit Intel® AMT Credentials** page.
2. View the `amtservice.log`, if an HTTP 401 error caused the system to fail, verify that the user name and password are correct on the **Edit Intel® AMT Credentials** page.
3. Verify that the domain and FQDN of the Intel® AMT system is correctly resolved from McAfee ePO.
4. Verify that the required Firewall Ports are allowed on the Intel® AMT system and McAfee ePO.

What happens if the Intel® AMT Power On action is executed on a system that is already running?

When McAfee ePO detects that the system is powered on, it does not execute the action.

Client tasks

What conditions are required to successfully execute the Client Tasks?

Make sure that these conditions are met:

- Client Tasks are enabled.
- Appropriate managed products are installed on the Intel® AMT system.
- Intel® AMT system is able to communicate with the Agent Handler within two minutes of restarting your system using the Power On action or Alarm Clock task.
- Intel® AMT system is able to boot from a powered off state if the Power On action or Alarm Clock task is performed from McAfee ePO.

The client tasks fail if the system is in a state of hibernation or standby.

How do I return the Intel® AMT system to its previous power state at the end of a Client Task Execution?

It is possible to shut down the Intel® AMT System after the system has started due to Power On action or Alarm Clock task. A McAfee ePO user can provide a `shutdown.exe` as an arbitrary command in the Client Task Execution policy. The previous power state is unknown, so the administrator must select a power state for the system.

Why were the Client Tasks not implemented on an Intel® AMT system that turned on using the Power On action or Alarm Clock task?

- The Agent Handler is not reachable.
- The Intel® AMT system fails to communicate with the Agent Handler within two minutes of restarting using the Power On action or Alarm Clock task, or if tasks were not present on the system.

How can I implement multiple arbitrary commands through a Client Task execution policy?

You can execute multiple arbitrary commands using a Windows batch file. The batch file, containing multiple commands, can be added to the Client Task Execution policy, which will be executed after the system starts either through the Intel® AMT turn on or through the Scheduled Alarm Clock.

To run a batch file, select `<System32>\cmd.exe` from **Run the following Command afterward** and enter `/c <path of your batch file>` in **Additional Parameters**.

It is necessary to add `@echo` as the first command in the batch file, otherwise the command added in the batch file is not executed.

Intel® AMT console

How do I send a Fast Call for Help from my Intel® AMT system?

See the system documentation on how to send a Fast Call for Help from the Intel® AMT System hardware, or open **Intel® Management and Security Status** and click **Get Technical Help to send a Fast Call**.

How do I access the Intel® MEBX BIOS?

Restart your system and press a combination of keys as defined by the manufacturer. For certain OEMs, press **Left Ctrl + P** until you hear a beeping sound. The default MEBX password is `admin`.

How do I access the web interface from an Intel® AMT System?

If the web interface is enabled on the Intel® AMT system, open Internet Explorer, type `https://<FQDN of the AMT System>:16993/`, and provide your Active Directory logon credentials or digest credentials added in the configuration profile.

The registry must be updated to allow Internet Explorer to connect to Port 16993. See http://support.microsoft.com/kb/908209 for the required registry changes.

Are there any other tools that can be used to check the status of the Intel® AMT system?

You can use these tools:

- Intel® Management and Security Status (IMSS)
- ACUconfig status or SystemDiscovery

Properties

When does the Last *Power On* Time parameter get updated on the Deep Command tab?

Last Power On Time is one of the properties displayed on the **Deep Command** tab of the **System Details** page. This property is updated when an Intel® AMT *Power On* action is executed from the McAfee ePO console.

Why are the Intel® AMT system properties not updated in a configured system?

Like other managed products, Intel® AMT properties appear after the second agent-server communication.

Local Access and *Remote Access*

What is the 63-character restriction warning message that appears while creating a Local Access Policy?

The Intel® AMT chipset limits the Local Access and Remote Access configuration to 63-characters. Out of them, 20-characters are used for the protocol header and directory path. For a Local Access policy to be successfully enforced, the actual Agent Handler name (published DNS or computer name) is shown in the drop-down list. The Local Access policy port number must be 43 characters or fewer. If the length is greater than 43 characters, a warning message is displayed and the policy can't be saved.

If the total FQDN size of the agent and Agent Handler exceeds 63 characters and the policy is enforced, the Local Access request sent by the Intel® AMT system doesn't work properly.

Alarm Clock

How do I verify that the Alarm Clock Policy is successfully enforced on an Intel® AMT system?

Verify these conditions:

- The Policy Enforcement task in the server task log shows the status as **completed**.
- From the **System Properties Intel® AMT** page, confirm that the alarm is enabled and time fields display the updated values.
- In the Intel® AMT system, the Alarm Clock values set by the Alarm Clock policy enforcement can be verified by using Intel® tools like Manageability Commander Tool and Powershell.

Configure or unconfigure

Can I unconfigure an Intel® AMT system using an Intel® RCS server other than the one that configured it?

Yes, but only when both the Intel® RCS servers belong to the same domain. When multiple Intel® RCS servers are configured within a domain, any of the servers can be used to configure or unconfigure an Intel® AMT system because they all share domain rights.

How do I unconfigure an Intel® AMT system manually?

1. Start your Intel® AMT system and invoke the MEBX screen.
2. Log on to the Intel® AMT system with the MEBX password (which might be different from the Admin password).

3 Locate and select the **Unconfigure Network Access** option.

A warning message states that the configuration is reset to the default values appears.

4 Press **Y** to continue.

5 On the next screen, select an appropriate option: **Full Unconfigure** or **Partial Unconfigure**, then press **Enter** to execute the configuration.

6 Once the unconfiguration is complete, the menu appears. Press **Return** to go back to the previous screen and press **Y** to exit the MEBX menu.

McAfee KVM Viewer

I started an IDE-R session through McAfee KVM Viewer and closed the screen. Why the IDE-R connection is still active when I reopen the McAfee Viewer screen?

An active IDE-Redirection session does not end when the McAfee KVM Viewer is closed. In the McAfee KVM Viewer screen, click **Tools** | **Power Control** | **End IDER Session** to end the IDE-R session.

General

Should I connect Intel® AMT systems to AC power to allow Intel® AMT actions?

Laptop devices with Intel® AMT support must be connected to an AC power supply. Detection of AC (normal power supply) operation and DC power (battery) operation is supported. If the laptop is on, the AC power supply can be disconnected. ePO Deep Command can communicate with the chipset on the laptop. However, if the laptop is turned off or in a different power state, the AC power supply must be connected to communicate with ePO Deep Command.

More details on the supported power packages are available in the Intel® AMT Release 2.5/2.6/4.x/6.x/7.0:

- http://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/DOCS/Implementation%20and%20Reference%20Guide/WordDocuments/supportformultiplepowerpolicies.htm
- http://software.intel.com/en-us/articles/mobile-computing-with-intel-amt/

Why do some of the interface items in certain forms are not aligned properly?

Make sure that you do not run your web browser in Compatibility Mode. McAfee ePO does not support this mode of the web browsers.

A Additional information

See these topics for more information that you may require to set up or manage ePO Deep Command.

Contents

- *Create a configuration profile using Intel RCS*
- *Customize wireless retry settings*
- *Set up the environment for Microsoft CA authentication*
- *Intel® MEBX password format*
- *Validate permissions*
- *Self-signed configuration certificates*
- *Intel® AMT action logs*
- *Python scripts for ePO Deep Command*

Create a configuration profile using Intel RCS

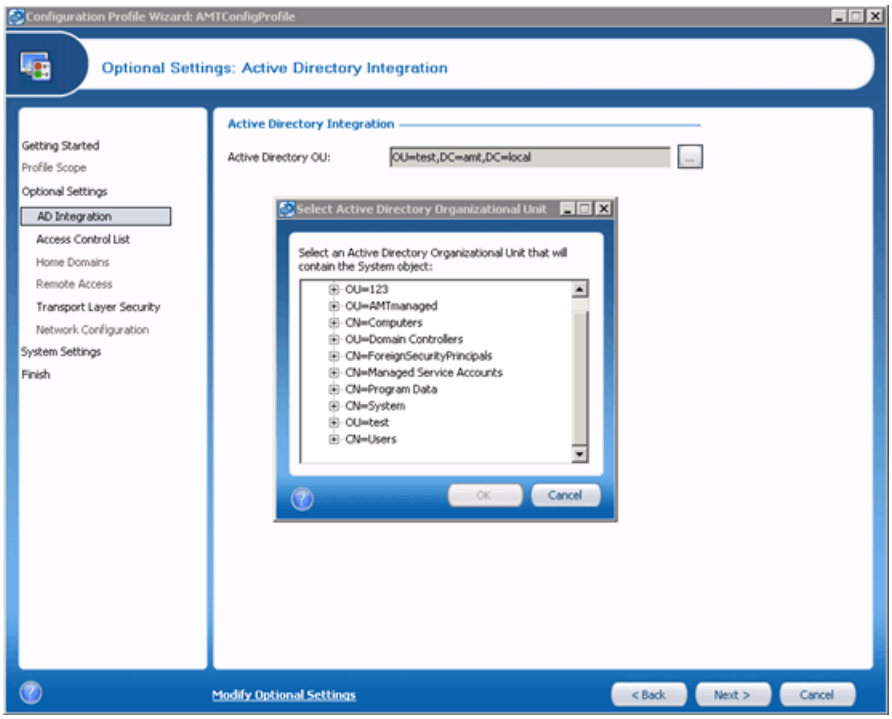
Create a configuration profile in the Intel® RCS server, for the settings required to push the Intel® AMT device configuration.

If you're using Microsoft CA certificates, see *Create a configuration profile that uses Microsoft CA certificates*.

Task

1. From the Intel® SCS Console, click the icon to create a profile, type a unique name, type any description, then click **OK** to open the **Configuration Profile** wizard.
2. On the **Getting Started** page, select **Configuration\Reconfiguration**, then click **Next**.
3. On the **Optional Settings** page, select these options, as needed, then click **Next**.
   - **Access Control List (ACL)** — To assign customized access levels to the systems based on users and groups.
   - **Transport Layer Security (TLS)** — To use the TLS protocol to encrypt and authenticate communication with the systems.
   - (Optional) **Active Directory Integration** — To use Kerberos authentication.
   - (Optional) **Network Configuration** — Select **WiFi Connection** suboption to allow wireless connections to the clients.

4 If using Digest authentication, skip to the next step. Otherwise, in the **Active Directory Integration** page, click … next to **Active Directory OU** and select the **Organizational Unit** where the system is stored in the Active Directory, then click **Next**.



During configuration, the Intel® SCS sends a request to the AD to create an object representing the Intel® AMT system and adds it to the **Active Directory Organizational Unit** (ADOU) that you define.

5 On the **Access Control List** (ACL) page, click **Add**, perform these options, as needed, in the **User/Group Details** page, then click **Next**:

a For **User Type**, select **Digest User** to use Digest authentication, or **Active Directory User/Group** to use Kerberos authentication, as needed.

b Provide credentials for the selected authentication type:

- For **Digest User**, type the user name and password.

  These Digest user credentials must be the same as the Intel® credentials in **Server Settings**.

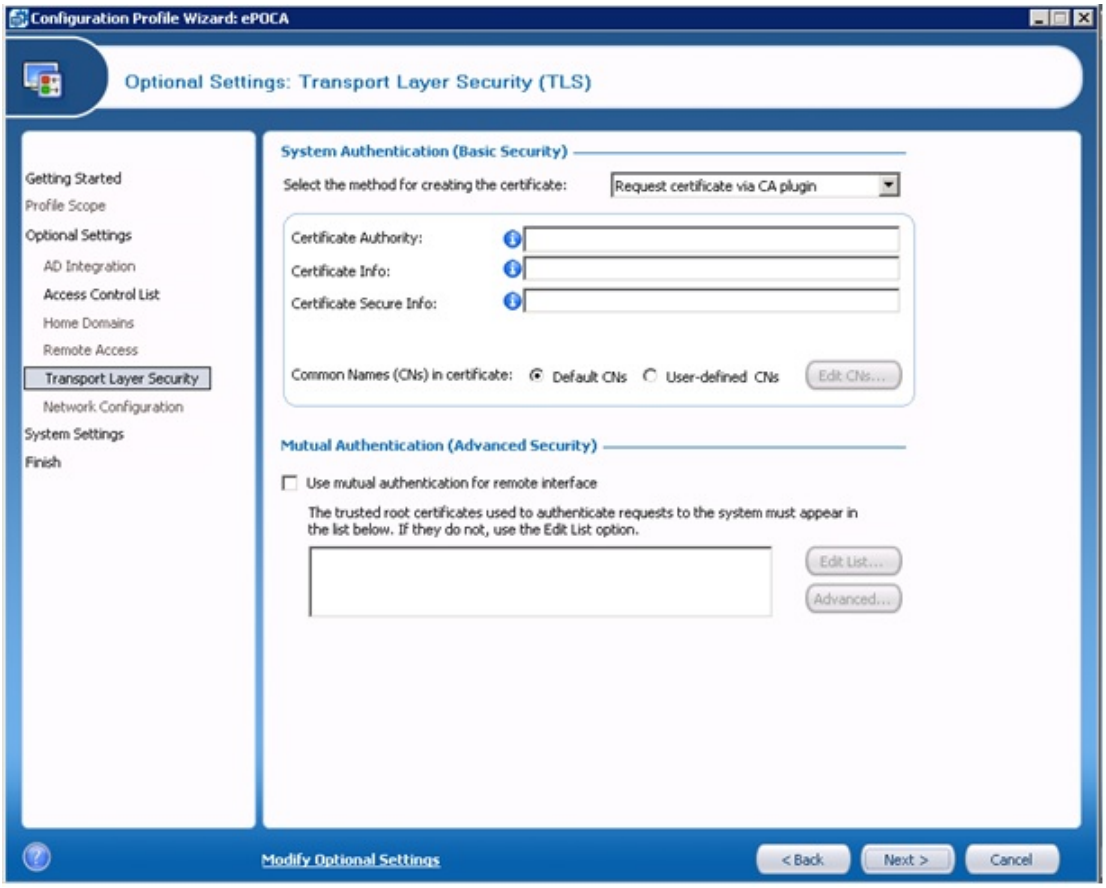
- For **Active Directory User/Group**, click **Browse**, then select a domain user or group.

c From the **Access Type** drop-down list, select **Both**.

d For **Realms**, select **PT Administration**, then click **OK**.

6 On the **Transport Layer Security** (TLS) page, select **Request certificate via CA plugin** to configure the profile that recognizes McAfee ePO Deep Command Root CA certificates, complete the options as needed, then click **Next**.

If the **Request certificate via CA plugin** method is not listed, make sure that the support for CA mediation is enabled in SCSConsole.exe.config. See *Enable McAfee ePO Deep Command certificates support in Intel RCS* for instructions.



a (Optional) In **Certificate Authority**, type a name for the McAfee ePO Deep Command Root CA.

b (Optional) In **Certificate Info**, type a description for the McAfee ePO Deep Command Root CA.

c (Optional) In **Certificate Secure Info**, provide credentials to access the McAfee ePO Deep Command Root CA in this format:

`-u <domain_name>\<user_name> -P <password>` (For example, `-u vprodemo \Administrator -P xxxxxxxx`.)

d From the **Common Names (CNs) in certificate subject name**, select **Default CNs**.

We recommend that you don't select **Use mutual authentication for remote**. When an Intel® AMT system is configured using a profile that uses both local and remote Mutual Authentications, the Remote Access policy enforcement to the client might fail.

7 On the **Network Configuration** page, perform these steps to set up wireless connections, then click **Next**.

a Select **Allow WiFi connection with the following WiFi setups**, then click **Add** to open the **WiFi Setup** screen.

b In the **Setup Name** field, enter a name for the Wi-Fi setup. The setup name can be up to 32 characters, and must not contain (/ \ < >: ; * |? ”) characters.

c In the **SSID** field, enter the Service Set Identifier (up to 32 characters) that identifies the specific Wi-Fi network. If left empty, the device tries to connect to all Wi-Fi networks that use Data Encryption as defined in this Wi-Fi Setup.

d From the **Key Management Protocol** drop-down list, select one of these options:

- **WiFi Protected Access (WPA)**
- **Robust Security Network (RSN)**

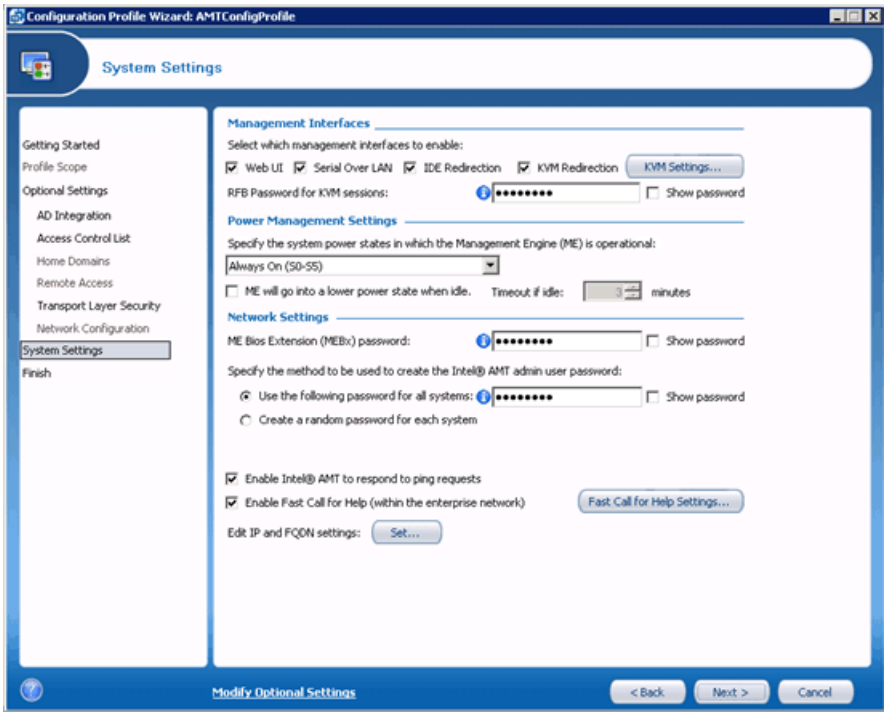
e From the **Encryption Algorithm** drop-down list, select one of these options:

- **Temporal Key Integrity Protocol (TKIP)**
- **Counter mode CBC MAC Protocol (CCMP)**

f Under **Authentication**, select **Passphrase**, type a password to establish the Wi-Fi connection, then retype it to confirm.

These settings are required to establish connection to wireless Intel® AMT systems. However, the client must have a wired connection during the configuration process.

8 On the **System Settings** page, complete the options, as needed, then click **Next**.



a In **Management Interfaces**, select all these options:

- **Web UI**
- **Serial Over LAN**

- **IDE redirection**
- **KVM redirection**

b In **Power Management Settings**, select **Always on (S0-S5)**.

c In **Network Settings**, type the password for locally accessing the MEBX settings (default is *admin* on a new system).

If you want to use mixed mode and created a password in **Edit Server Settings** to support host-based configuration, type the same password in this field.

d Select **Enable Intel® AMT to respond to ping requests** and **Enable Fast Call for Help (within the enterprise network)**.

9 Click **Finish** to close **Configuration Profile** wizard.

The profile is added to the list of profiles.

Customize wireless retry settings

Retries are implemented to establish a connection to perform Intel® AMT actions on a wireless client.

By default number of retries are three times and retry delay is 5 seconds. You can override these values by performing this task.

Task

For option definitions, click **?** in the interface.

1 Close the McAfee ePO console, stop Application and Server services, then browse to this directory:

```
<Installation Directory>\McAfee\ePolicy Orchestrator\DB
```

(Replace <Installation Directory> with the McAfee ePO installation directory)

2 Open notepad and type the following content:

```
[Connection]
RetryCount=<0 to 10>
RetryDelay=<1000 to 15000 miliseconds>
MeSwitchDelay=<20000 to 180000 miliseconds>
```

(Replace the values as needed)

3 Save the file as .ini (for example, `edc.ini`).

4 Start the McAfee ePO Application and Server services, then perform an Intel® AMT action on a client from the McAfee ePO console.

To validate the changes, check `AMTService.log` for an entry similar to the following:

Read <file_name>.ini for retry overrides

Retry Count is <Number of Retries>

Retry Delay is <Interval in milliseconds>

ME Switch Delay is <Interval in milliseconds>

Set up the environment for Microsoft CA authentication

To use certificates generated by Microsoft CA, perform these tasks in addition to the other mandatory tasks for setting up ePO Deep Command.

We recommend that you use certificates generated by ePO Deep Command root CA to simplify the configuration process. If you're using Microsoft CA for your environment, use it only for remote configuration.

- (Optional) If your enterprise CA is located in a different domain than McAfee ePO, import CA certificates to the certificate store of McAfee ePO.
- (Optional) If you need chain of certificates for authentication, create a certificate chain to import.
- Import Microsoft CA certificates to McAfee ePO.
- Create a certificate template.
- Enable the certificate template.
- Issue certificates automatically.
- Create a configuration profile that uses Microsoft CA to create certificates.
- (Optional) If you're using ePO Deep Command Gateway services, generate Microsoft CA certificates to use with the Stunnel configuration.

Tasks

- *Import certificates to server* on page 151
  In an environment where McAfee ePO is deployed across different domains, import Microsoft CA certificates to the system where McAfee ePO or Agent Handler is installed.
- *Create a certificate chain* on page 151
  You can copy the root and intermediate certificates to a single file and save it as a Privacy Enhanced Mail (PEM) file.
- *Import certificates to McAfee ePO* on page 152
  Import and activate Microsoft CA certificates to McAfee ePO.
- *Create a certificate template* on page 152
  Create a remote configuration certificate template for the Intel® AMT configuration when you're using self-signed CA certificates.
- *Enable the certificate template* on page 154
  Enable the certificate template that you created for Intel® AMT configuration.
- *Issue certificates automatically* on page 154
  Configure to issue certificates automatically to avoid sending the certificate requests to "pending" queue.
- *Create a configuration profile that uses Microsoft CA certificates* on page 154
  When you're creating a profile, select the Microsoft CA option as a method for creating certificates.
- *Generate certificates for Stunnel using Microsoft CA* on page 156
  Generate certificates from Microsoft CA to use with Stunnel configuration.

Import certificates to server

In an environment where McAfee ePO is deployed across different domains, import Microsoft CA certificates to the system where McAfee ePO or Agent Handler is installed.

Before you begin

- Perform this task only if McAfee ePO is not in the same domain with enterprise CA\PKI.
- Specify ePO Deep Command credentials and import the Server Authentication Certificate in McAfee ePO.

In an enterprise CA\PKI, the Microsoft directory service automatically replicates the root or intermediate certificates. If it's a standalone CA or non-Microsoft PKI, and if the required certificates are not available, perform this task. This prevents 401 or 12175 errors from being displayed in the `AMTService.log` file.

When you use Internet Explorer to install the certificate to your Trusted Roots certificate store, it affects only the current user's certificates and not the local system. Users must use the Microsoft Management Console certificates to install on the local system or a service account. You must be check in these certificates to **Trusted Root Certification** and **Intermediate Certification Authorities**, then restart the McAfee ePO services.

These instructions are specific to importing the root or intermediate certificate of the CA that was used for creating and signing the Server Authentication Certificate.

Task

For option definitions, click **?** in the interface.

1. On the McAfee ePO server, run `mmc` from the command prompt.
2. Select **File** | **Add/Remove Snap-in**, then click **Add**.
3. In **Add Standalone Snap-in**, select **Certificates**, then click **Add**.
4. From the **Certificates snap-in** page, select **Computer Account**, then click **Next**.
5. From the **Select Computer** page, select **Local Computer**, then click **Finish**.
6. Click **Close**, then click **OK**.
7. Go to **Console Root** and expand **Certificates (Local Computer)**, then expand **Trusted Root Certification Authorities**. The **Certificates** folder must be displayed in the right pane. Right-click **Certificates**, then click **all Tasks** | **Import**.
8. In the Certificate Import wizard, click **Next**, then **Browse** and select the CA Certificate. Make sure that **Trusted Root Certification Authorities** is where the certificate is stored. Click **Next**, then click **Finish** to complete the certificate importing process.
9. Go to **Console Root** and expand **Certificates (Local Computer)**, then expand **Intermediate certification Authorities**. The **Certificates** folder must be displayed in the right pane. Right-click **Certificates**, then click **all Tasks** | **Import**.

Create a certificate chain

You can copy the root and intermediate certificates to a single file and save it as a Privacy Enhanced Mail (PEM) file.

This task is required only when you're using remote configuration and to use a chain of certificates for server authentication.

Task

1 On the Certificate Authority server, click **Start** | **Programs** | **Administrative Tools** | **Certification Authority**.

2 From the **Console Root** tree, right-click the certificate, then select **Properties**.

3 On the **Properties** page, click the **General** tab, then click **View Certificate**.

4 On the **Certificate** page, click the **Details** tab, then click **Copy to File**.

5 On the **Certificate Export Wizard** page, click **Next**, select the export file format as **Base-64 encoded X.509 (.CER)**, then click **Next** again.

6 Specify the name of the file to export, click **Next**, then click **Finish**.

7 With a text editor (such as WordPad), copy and paste the entire body of the certificate into one text file.

8 If intermediate certificates exist within your environment, follow the steps 2 through 6 for each certificate, then copy the entire text between "Begin" and "End" statements and place in bottom-to-top order (root at the last) in the text file that you created in step 7.

9 Save the combined file as a .PEM file.

Import certificates to McAfee ePO

Import and activate Microsoft CA certificates to McAfee ePO.

Task

You can import a single or chain of certificates. For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Configuration** | **Server Settings**.

2 In **Setting Categories**, select **Intel® AMT Credentials**, then click **Edit** to modify your ePO Deep Command settings.

3 In **Trusted Root Certificates**, click **Import Certificate/Key**, browse to select a PEM encoded (.pem file), DER encoded (.der file), or a PKCS12 (.p12 file) for a certificate or chained certificates, click **Next**, then click **Save**.

   The certificate gets listed in the **Trusted Root Certificate** box.

4 Select the certificate imported, click **Activate**, then click **Save**.

See also

Modify ePO Deep Command settings on page 26

Create a certificate template

Create a remote configuration certificate template for the Intel® AMT configuration when you're using self-signed CA certificates.

Perform this task only when you're using self-signed CA certificates.

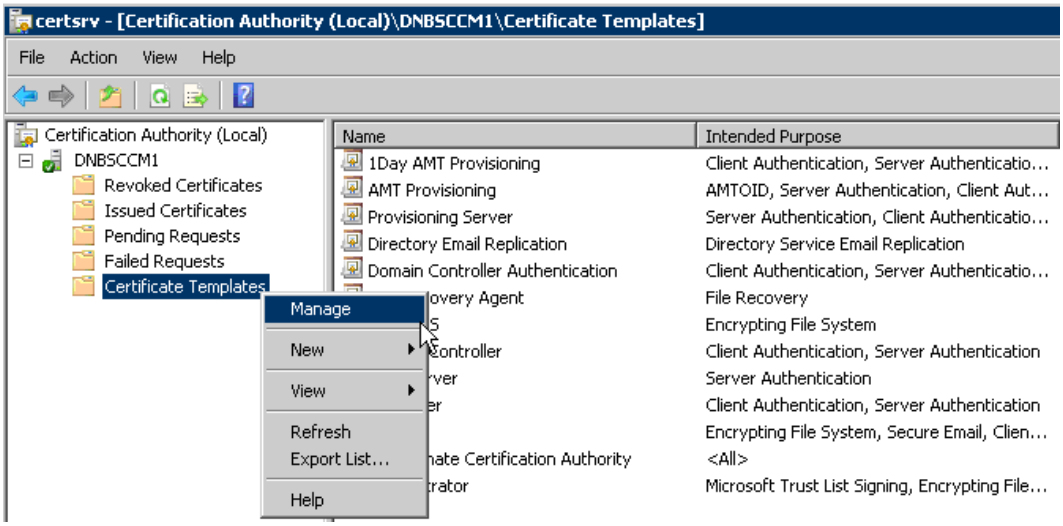
Task

1 In the Certificate Authority server, click **Start** | **Programs** | **Administrative Tools** | **Certification Authority**.

2 From the **Console Root** tree, double-click **Certificate Templates**.

   The list of templates appear in the right pane.

3 Right-click the **Certificate Templates** and select **Manage**.



4 In the right-pane, right-click the **Computer** template and select **Duplicate Template** to open the **Properties** page.

5 In **Template display name**, type a name for the template (for example, `AMT Configuration`).

6 Click the **Extensions** tab, select **Application Policies**, then click **Edit**:

   a Click **Add**, then click **New**.

   b Enter the policy name as `AMT OID`, and in the **Object Identifier (OID)** field enter this:

   `2.16.840.1.113741.1.2.3`

   c Click **OK** three times to return to the **Properties of New Template** window.

7 Click the **Subject Name** tab, then select **Supply in the request**.

8 Click the **Request Handling** tab, then select **Allow private key to be exported**.

9 Click **OK**.

See also

Self-signed configuration certificates on page 160

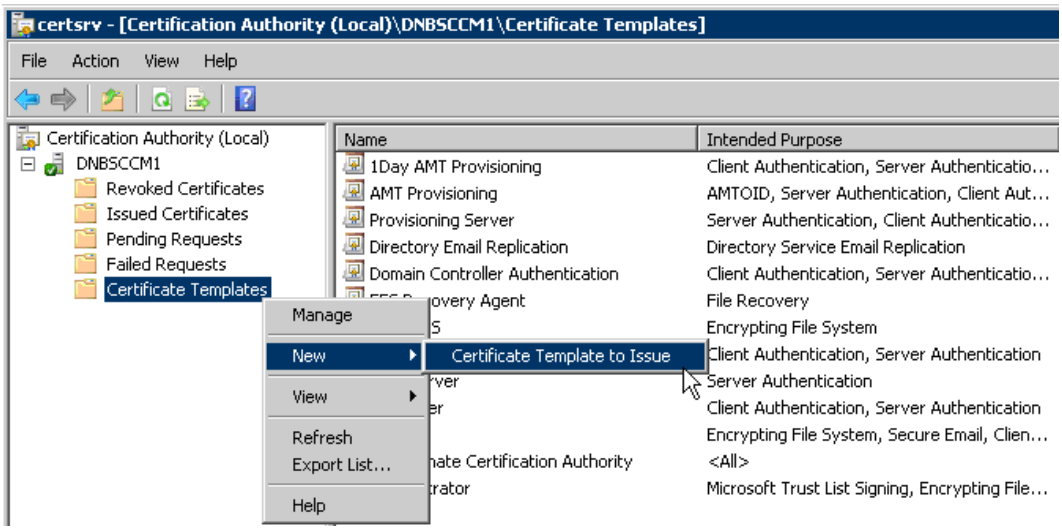
Enable the certificate template

Enable the certificate template that you created for Intel® AMT configuration.

Task

1 In the Certificate Authority server, click **Start** | **Programs** | **Administrative Tools** | **Certification Authority**.

2 From the **Console Root** tree, select **Certificate Authority** | **Certificate Templates**. Right-click the right pane and select **New** | **Certificate Template to Issue**.



3 In the **Enable Certificate Templates** screen, select a template to use, then click **OK**.

The template now appears in the right pane with the other certificate templates.

Issue certificates automatically

Configure to issue certificates automatically to avoid sending the certificate requests to "pending" queue.

ePO Deep Command doesn't support pending certificate requests. If during configuration, the CA puts the certificate into the "Pending Requests" state, Intel® SCS returns an error (#35).

Task

1 In the Certificate Authority server, click **Start** | **Programs** | **Administrative Tools** | **Certification Authority**.

2 Right-click the CA and select **Properties**.

3 Click the **Policy Module** tab, then click **Properties**.

4 In the **Request Handling** tab, select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**, then click **OK**.

Create a configuration profile that uses Microsoft CA certificates

When you're creating a profile, select the Microsoft CA option as a method for creating certificates.

If you're using McAfee ePO Deep Command root CA certificates, see *Create a configuration profile*.

Task

1 From the Intel® SCS Console, click the icon to create a profile and to open the **Configuration Profile** wizard.

2 In **Profile Description**, enter a unique name, then click **Next**.

3 In **Optional Settings**, select **Access Control List (ACL)**, **Transport Layer Security (TLS)**, and **Active Directory Integration** (if using Kerberos authentication), then click **Next**.

4 If using Digest authentication, skip to the next step. Otherwise, in the **Active Directory Integration** page, click … next to **Active Directory OU** and select the **Organizational Unit** where the system is stored in the Active Directory, then click **Next**.

> During configuration, the Intel® SCS sends a request to the AD to create an object representing the Intel® AMT system and adds it to the **Active Directory Organizational Unit** (ADOU) that you define.

5 On the **Access Control List** (ACL) page, click **Add**, then perform these steps on the **User/Group Details** page:

- **a** For **User Type**, select **Digest User** to use Digest authentication, or **Active Directory User/Group** to use Kerberos authentication, as needed.
- **b** Provide credentials for the selected authentication type:
  - For **Digest User**, type the user name and password.
  - For **Active Directory User/Group**, click **Browse**, then select a domain user or group.
- **c** From the **Access Type** drop-down list, select **Both**.
- **d** For **Realms**, select **PT Administration**, then click **OK**.

6 On the **Transport Layer Security** (TLS) page, select **Request certificate from Microsoft CA**, then perform these steps as needed, then click **Next**.

- **a** In **Certificate Authority**, select the Microsoft Certification Authority server to be used.
- **b** From the **Server Certificate Template**, select the required certificate template. Click **Refresh CAs & Templates** if the newly created template is not getting populated..
- **c** From the **Common Names (CNs) in certificate subject name**, select **Default CNs**.

> We recommend that you don't select **Use mutual authentication for remote**. When an Intel® AMT system is configured using a profile that uses both local and remote Mutual Authentications, the Remote Access policy enforcement to the client might fail.

7 On the **System Settings** page, perform these steps as needed, then click **Next**.

- **a** In **Management Interfaces**, select all these options:
  - **Web UI**
  - **Serial Over LAN**
  - **IDE redirection**
  - **KVM redirection**
- **b** In **Power Management Settings**, select **Always on (S0-S5)**.

c In **Network Settings**, type Intel® ME BIOS Extension (MEBX) password for locally accessing the MEBX settings (default is *admin* on a new system).

> If you want to use mixed mode and created a password in **Edit Server Settings** to support host-based configuration, type the same password in this field.

d Select **Enable Intel® AMT to respond to ping requests** and **Enable Fast Call for Help (within the enterprise network)**.

8 Click **Finish** to close **Configuration Profile** wizard.

The profile is added to the list of profiles.

See also

Create a configuration profile using Intel RCS on page 145

Generate certificates for Stunnel using Microsoft CA

Generate certificates from Microsoft CA to use with Stunnel configuration.

Before you begin

The steps that follow provide an example of the process used to generate the certificate. For complete instructions on generating certificates, go to http://www.stunnel.org/?page=howto and see *Generating the Stunnel certificate and private key (.pem)*.

> You can generate certificates on another system to avoid copying certification-dependent software, executables, or binaries on the DMZ.

> Don't perform this task if you're using the McAfee ePO Deep Command Root CA.

When you generate Stunnel certificates, follow these guidelines:

- The private key size must not exceed 2048.
- Don't include an email address.
- Make sure that you enter the fully qualified domain name of the ePO Deep Command Gateway server.
- Make sure that the Web Server template is used when the certificate request is submitted for signing by the CA.

Task

For option definitions, click **?** in the interface.

1 Open a web browser, then access the CA server URL.

The CA server URL must include the server's FQDN followed by `/certsrv`. For example, *http://<Server FQDN>/certsrv*.

2 Log on to the CA server as a domain administrator, click **Request a Certificate** | **Advanced Certificate Request**, then click **Create and submit a request to this CA**.

3 Select the template created, the FQDN of the host system to install Stunnel, type a name, then click **Submit**.

4 Click **Install this certificate**.

The certificate gets listed under **Personal certificates** for current user on the host.

5 Select certificate and export with private key.

6 Select **Include all certificates in the certification path.**

7 Type a password, then save the file as with `.pfx` extension.

For example, `test.pfx`.

8 Run these commands to create certificate files.

```
openssl pkcs12 -nocerts -in C:\test.pfx -out C:\cira.key -nodes
openssl pkcs12 -clcerts -nokeys -in C:\test.pfx -out C:\cira.pem -nodes
openssl pkcs12 -cacerts -nokeys -in C:\test.pfx -out C:\ca.cer -nodes
```

Replace `C:\test.pfx` with the actual file path and its name.

The three required files, `cira.key`, `cira.pem`, and `ca.cer`, are created.

9 Copy the certificate files to the Stunnel installation directory. For example, `C:\Program Files (x86)\stunnel`.

Intel® MEBX password format

When you change Intel® MEBX password, consider these requirements.

- The password length must be at least eight characters long.
- It must contain at least one numerical character. For example, '0', '1',...'9'.
- It must contain at least one 7-bit ASCII non-alphanumeric character. For example, '!', '$', ';'.
- It must not contain '"', '\', ',' and ':'.
- It must contain both lowercase Latin ('a', 'b', ...'z') and uppercase Latin ('A', 'B',...'Z'), or non-ASCII characters (UTF+00800 and above).

Validate permissions

When you deploy the RCS Manager plug-in to Intel® RCS systems, it automatically applies the required permissions to add Domain Computers in WMI and DCOM permissions. However, if these changes are not applied due to some environmental restrictions, apply them manually.

Tasks

- *Modify WMI permissions to add domain computers* on page 157
  The remote configuration of Intel® AMT systems requires appropriate WMI permissions for domain computers on the server where the Intel® RCS is installed and configured.
- *Modify DCOM permissions to add domain computers* on page 159
  The configuration process requires appropriate DCOM permissions for domain computers in the server where the Intel® RCS is installed and configured.

Modify WMI permissions to add domain computers

The remote configuration of Intel® AMT systems requires appropriate WMI permissions for domain computers on the server where the Intel® RCS is installed and configured.

Perform this task for each required user group.

Task

For option definitions, click **?** in the interface.

1 Click **Start** | **Administrative Tools**, then click **Server Manager**.

2 Expand **Configuration**, right-click **WMI Control** and select **Properties**.

3 Go to the **Security** tab,

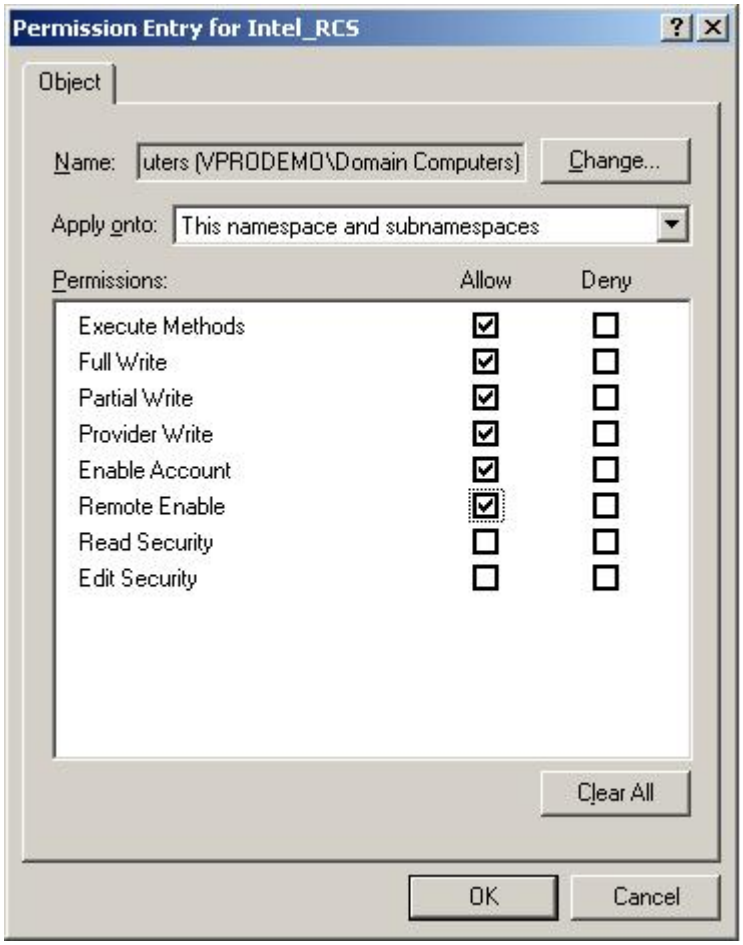
a From the tree, select **Intel_RCS**, then click **Security**.

b Click **Advanced**, add the user group as needed (for example, **Domain Computers**), then double-click the permission entry for the selected user group.

Make sure that all required users are added to this domain.

c Select **This namespace and subnamespaces** under **Apply to**, then allow these permissions.

- **Execute Methods**
- **Full Write**
- **Partial Write**
- **Provider Write**
- **Enable Account**
- **Remote Enable**



4 Save the settings and close the properties screens.

Modify DCOM permissions to add domain computers

The configuration process requires appropriate DCOM permissions for domain computers in the server where the Intel® RCS is installed and configured.

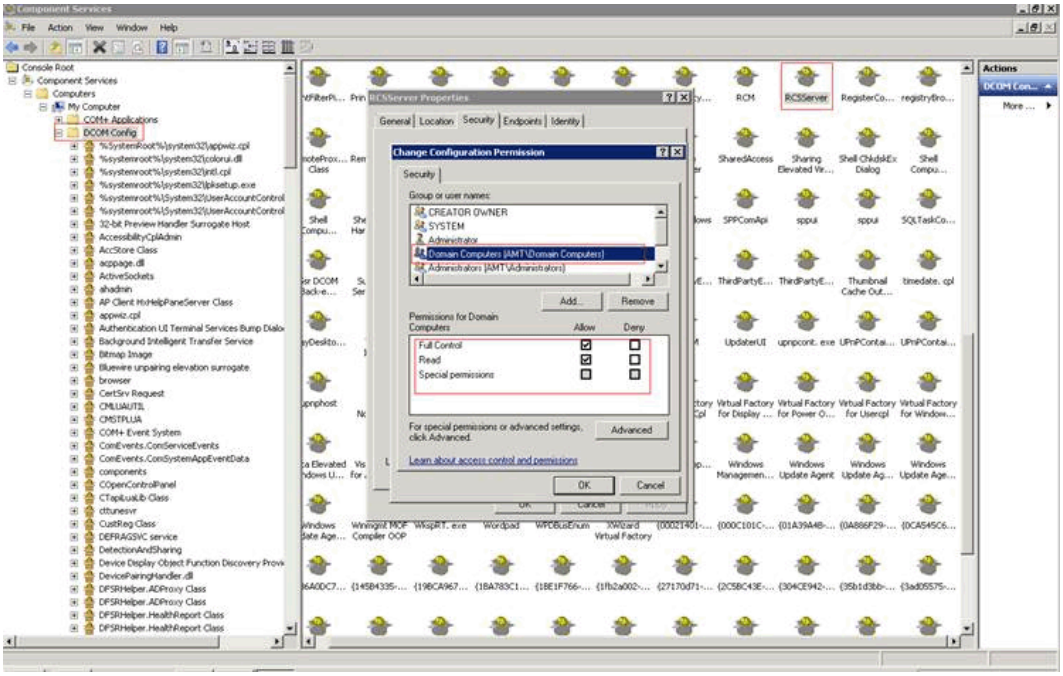
Task

For option definitions, click **?** in the interface.

1. Click **Start** | **Run**, then type `dcomcnfg` and press **Enter**.
2. Expand **Console Root** | **Component Services** | **Computers**, right-click **My Computer**, then select **Properties**.
3. Click the **COM Security** tab.
4. In **Access Permissions**,
   a. Click **Edit Limits**.
   b. Add **Domain Computers** if it's not listed, select **Domain Computers** and allow these permissions for the **Domain Computers** group, then click **OK**.
      - **Local Access**
      - **Remote Access**
5. In **Launch and Activation Permissions**,
   a. Click **Edit Limits**.
   b. Add **Domain Computers** if it's not listed, select **Domain Computers** and allow these permissions for the **Domain Computers** group, then click **OK**.
      - **Local Launch**
      - **Remote Launch**
      - **Local Activation**
      - **Remote Activation**
6. Click **OK** again.
7. (Optional) If the Intel® RCS is running on a Microsoft Windows 2008, perform these steps on the **Component Services** page:
   a. Expand **Console Root** | **Component Services** | **Computers** | **My Computer** | **DCOM Config**, right-click the entry for the Intel® RCS, then select **Properties**.
   b. On the **Security** tab, under **Configuration Permissions**, select **Customize**, then click **Edit**.

c Add **Domain Computers** if it's not listed, then allow these permissions for the **Domain Computers** group.

- **Full Control**
- **Read**
- **Special Permission**



8 Close the **Component Services** page.

Self-signed configuration certificates

When using self-signed Certification Authority to create the configuration certificate, consider these points.

- Its root hash must be entered into each AMT system that is configured. It can be done at the time of manufacture or entered manually using the Intel® Management Engine BIOS Extension interface.
- A certificate template must be created first. The computer template available in the Microsoft Certification Authority can be duplicated.
- The Object Identifier 2.16.840.1.113741.1.2.3 must be added in the **Enhanced Key Usage** section of the template.
- A certificate request is sent to the self-signed CA with the FQDN of the configuration server in the Subject Name.
- The CA uses this template to generate the certificate, which is then saved on the configuration server.

Intel® AMT action logs

Here is the information about the feature-wise list of log entries created as a result of Intel® AMT actions.

Table A-1 Server Task Log entries

Feature	Server Task Log entry	Description
SOL (Serial-over-LAN)	Initiated Start of Serial-over-LAN session	Added when SOL is initiated, with the status: • In Progress — A session is active. • Completed — A session finished successfully. • Failed — A session fails. • Terminated — A session is closed.
	Initiated Stop of Serial-over-LAN (SOL) session	Added when SOL stop is initiated, with the status: In Progress, Completed, Failed, or Terminated.
IDE-R	Start /Reboot with Options	Added when IDE-Redirection (IDE-R) is initiated, with the status: In Progress, Completed, Failed, or Terminated.
	Initiated Stop of Image Redirection	Added when IDE-R stop is initiated, with the status: In Progress, Completed, Failed, or Terminated.
SOL BIOS	Boot/Reboot to BIOS Setup	Added when Boot/Reboot to BIOS Setup is initiated, with the status: In Progress, Completed, Failed, or Terminated
Power On	Initiated Out-of-Band *Power On*	Added when Out-of-Band *Power On* is initiated, with the status: In Progress, Completed, Failed, or Terminated.
Policy Enforcement	Out-of-Band Enforce AMT Policies	Added when Enforce AMT Policies action is initiated, with the status: In Progress, Completed, Failed, or Terminated.
Normal Boot/Restart	Initiated Normal Boot/ Reboot	Added when Normal Boot/Reboot is initiated, with the status: In Progress, Completed, Failed, or Terminated.
Run Tag Criteria	ePO Deep Command: Run Tag Criteria	Added when **ePO Deep Command: Run Tag Criteria** is initiated, with the status: Completed or Terminated.

Table A-2 Audit Log entries

Feature	Audit Log entry	Description
SOL	Serial-over-LAN (Request to Start Serial-over-LAN session sent to System)	Displays when SOL is initiated.
	Serial-over-LAN (Request to Stop Serial-over-LAN session sent to System)	Displays when SOL stop is initiated.
IDE-R	Initiated Boot/Reboot from Image	Displays when IDE-R is initiated.
	Initiated Stop of Image Redirection	Displays when IDE-R stop is initiated.
SOL BIOS	Initiated Boot/Reboot to BIOS Setup	Displays when Boot/Reboot to BIOS setup is initiated.
Power On	Out-of-Band *Power On*	Displays when Out-of-Band *Power On* is initiated.
Policy Enforcement	Out-of-Band Enforce AMT Policies	Displays when Enforce AMT Policies action is initiated.

Table A-2 Audit Log entries *(continued)*

Feature	Audit Log entry	Description
Normal Boot/Restart	Initiated Normal Boot/Reboot	Displays when Normal Boot/Reboot is initiated.
Run Tag Criteria	Evaluate AMT tag criteria	Displays when Evaluate AMT tag criteria is initiated.

Table A-3 Threat Event Log entries

Feature	Threat Event Log entry	Description
Local Access	Local Fast Call for Help	Intel® AMT system initiates a Local Access call.
Remote Access	Connected – Remote Fast Call for Help	Intel® AMT system initiates a Remote Access call.
	Disconnected – Remote Fast Call for Help	Intel® AMT system closes a Remote Access call.

Python scripts for ePO Deep Command

You can write Python scripts to enforce Intel® AMT policies and turn on your client systems from the Intel® AMT action using the McAfee ePO scripting.

See *McAfee ePolicy Orchestrator Scripting Guide* for more information on using Python scripts.

Download the python client

Download the Python Remote Client scripting library from McAfee ePO.

Task

For option definitions, click **?** in the interface.

1 In the McAfee ePO console, click **Menu** | **Software** | **Software Manager**.

2 In **Product Categories** under **Software (by Label)**, click **Management Solutions**.

3 Select **McAfee ePolicy Orchestrator 4.6** as the product, then click **Download** for the corresponding Python Remote Client.

Sample script for the *Power On* action

Here is a sample script to perform Power On action through the McAfee ePO Python Scripting support.

```
# Script to do an OOB Power On through the ePO Python Scripting support.
# The parameters to be passed to the script is an IP address or a list of comma-separated
IP addresses.

import mcafee
import sys
# mcafee.client() function in this command is using these parameters
# 1st parameter is the hostname of the McAfee ePO System.
# 2nd parameter is the port on which the McAfee ePO interface is accessible.
# 3rd parameter is the username that is used to log on to the McAfee ePO interface.
# 4th parameter is the password of the User name provided in the 3rd parameter.
# 5th parameter is always https and 6th parameter is always json.

mc = mcafee.client('myepo','8443','admin','epo', 'https','json')
try:
    input = sys.argv[1] #input to the script, our AMT system IP address.
except:
    print "Missing 1st parameter. Provide a single IP address of a comma-separated list of
```

```
IP address"
    print "Provide help as the first parameter to get more information"
else:
    if input == "help" or input == "-h" or input == "--h" :
        print "This script attempts to do a OOB Power On for a remote AMT system using
scriptable support in the ePO"
        print "It requires only one parameter. Pass the IP address of the remote AMT system
to do a Power On"
        print "You can optionally pass a comma-separated list of IP addresses of the remote
AMT  systems(s) to do a Power On"
        print "Example: c:\python26\python.exe oobpoweron.py amt01"
        print "NOTE: Run the command \"set PYTHONIOENCODING=utf-8\" on the command prompt
before running the oobpoweron.py script to be able to see the errors"
    else:
        try:
            result = mc.amt.powerOn(input)
        except mcafee.CommandInvokerError,e:
            try:
                print "Error in doing OOB Power on as the command failed to invoke properly
due to the following error"
                print "================"
                print e.__str__()
                print "================"
            except:
                print "NOTE: Run the command \"set PYTHONIOENCODING=utf-8\" on the command
prompt
before running the oobpoweron.py script to be able to see the errors"
        except AttributeError,e:
            print "Error in using amt.powerOn attribute"
```

Sample script for Intel AMT policy enforcement

Here is a sample script to enforce Intel® AMT policy through the McAfee ePO Python Scripting support.

```
# Script to do an OOB Power On through the ePO Python Scripting support.
# The parameters to be passed to the script is an IP address or a list of comma-separated
IP address.

import mcafee
import sys
# mcafee.client() function in this command is using these parameters
# 1st parameter is the host name of the McAfee ePO system.
# 2nd parameter is the Port on which the McAfee ePO interface is accessible.
# 3rd parameter is the User name that will be used to login to the McAfee ePO interface.
# 4th parameter is the Password of the User name provided in the 3rd parameter.
# 5th parameter is always https and 6th parameter is always json.

mc = mcafee.client('m0','8443','admin','epo', 'https','json')
try:
    input = sys.argv[1] #input to the script, our AMT system IP address.
except:
    print "Missing 1st parameter. Provide a single IP address of a comma-separated list of
IP address"
    print "Provide help as the first parameter to get more information"
else:
    if input == "help" or input == "-h" or input == "--h" :
        print "This script will attempt to do a OOB Policy Enforcement for a remote AMT
system
using scriptable support in the ePO"
        print "It requires only one parameter. Pass the IP address of the remote AMT system
to do a Power On"
        print "You can optionally pass a comma-separated list of IP addresses of the remote
AMT
 systems(s) to do a Policy Enforcement"
        print "Example: c:\python26\python.exe oobenforcepolicy.py amt01"
        print "NOTE: Run the command \"set PYTHONIOENCODING=utf-8\" on the command prompt
before
 running the oobenforcepolicy.py script to be able to see the errors"
    else:
        try:
            result = mc.amt.enforcePolicy(input)
        except mcafee.CommandInvokerError,e:
```

```
            try:
                print "Error in doing OOB Policy Enforcement on as the command failed to
invoke
properly due to the following error"
                print "================"
                print e.__str__()
                print "================"
            except:
                print "NOTE: Run the command \"set PYTHONIOENCODING=utf-8\" on the command
prompt
before running the oobenforcepolicy.py script to be able to see the errors"
        except AttributeError,e:
            print "Error in using amt.enforcePolicy attribute"
```

Index

A

actions
- AMT policies, enforcing 111
- boot/reboot to BIOS 107
- configuration policy, enforcing 111
- IDE-redirection 109
- image redirection, stopping 111
- normal boot/reboot 108
- over wireless 63
- power on 106
- serial-over-LAN 109
- user consent 107

AMT configuration
- action 111
- credentials, setting 48
- dcom permissions, adding manually 159
- host-based configuration 36, 94
- permissions, validating 157
- policy 49, 53, 94
- profile manager 10, 40
- remote configuration 38, 50, 94
- states 42
- third-party CA 150
- WMI permissions, adding manually 157

AMT unconfiguration
- identify state 55
- policy 55, 94
- tag removal 56

C

configuration profile
- template, importing 45
- through ePO console, creating 45
- through RCS console, creating 145, 154

D

dashboards and monitors
- benefits summary 82
- management summary 80
- RCS management summary 81
- readiness summary 81
- reporting summary 75

Deep Command
- action logs 161
- AMT actions 105
- AMT configuration overview 35
- AMT credentials, specifying 26
- AMT management 93
- AMT overview 9
- architecture 14
- certificate management 30
- components 10, 23
- events 115
- events, filtering 116
- extensions, installing 24
- extensions, removing 32
- extensions, upgrading 24
- forward events 116
- high-level workflow 14
- maintenance tasks 113
- overview 7
- policies 93
- process flow 13
- reports 69
- requirements 18
- Software Manager 23
- software, removing 31
- user permissions 28

Deep Command root CA
- certificates, exporting 30
- certificates, importing 30
- certificates, regenerating 30
- trusted root certificates 26

Discovery and Reporting
- dashboard 75
- overview 10
- plug-in, deploying 25
- plug-in, removing 32
- properties collection 85
- queries 69

E

error messages 129
- 401,12175 151

F

frequently asked questions 141

H

host-based configuration
- authentication 38
- client control mode 36
- move to admin control 95
- overview 36
- policy 49, 94
- user consent 37

K

KVM Viewer
- CA certificate, exporting 30
- certificate, adding snap-in 123
- certificate, copying 122
- certificate, importing 122
- connection, switching 126
- local connection 126
- options 127
- overview 10, 119
- policy 100
- policy, enforcing 121
- remote connection 126
- requirements 121
- settings 123
- software, downloading 121
- workflow 120

M

Management Framework
- client, deploying 26
- client, removing 32
- dashboard 80
- overview 10
- queries 71

P

policies
- alarm clock 96
- AMT 96
- automatic enforcement 112
- CILA 97
- CIRA 98
- client task execution 101
- client task log 102
- configuration 94
- KVM 100
- local access 97
- power on 96
- remote access 98
- server tasks 112

product features 7
Profile Management
- extension, installing 51
- overview 10

Python scripts
- AMT policy enforcement 163
- out-of-band power-on 162

Q

queries and reports
- filters 72
- management queries 71
- queries, viewing 71
- RCS management queries 71
- reporting 69

R

RCS Manager
- dashboard 81
- how it works 40
- package, checking in 51
- plug-in, deploying 52
- plug-in, removing 31
- queries 71

remote access
- certificates, validating 61
- gateway server, installing 58
- stunnel, configuring 60

remote configuration
- admin control mode 38
- authentication 40
- move from client control 95
- overview 38
- policy 53, 94
- prerequisites 50
- Profile Manager 40
- Profile Manager, installing 51
- RCS Manager, check-in 51
- root CA 41
- tasks 50
- third-party CA, enabling 51
- TLS 41
- vendor-supplied certificates 41

requirements
- AMT versions 20
- KVM Viewer 121
- operating system 19
- ports 21
- software 19
- system 18
- upgrade 20

S

server tasks
- AMT policies, enforcing 112
- AMT tag, assigning 25
- power on 112

T

third-party CA
- authentication, setting up 150
- certificate chain, creating 151
- certificate issuance 154
- certificate snap-in, adding 151
- certificates, activating 152
- certificates, importing 152
- configuration profile, creating 154
- remote access, setting 156
- stunnel certificates, generating 156
- template, creating 152
- template, enabling 154

U

user consent
- boot/reboot to BIOS 107
- code, generating 107
- host-based requirement 37
- IDE-redirection 109
- KVM redirection 126

W

wireless
- configuration profile, creating 65, 145
- KVM Viewer settings 123
- overview 63
- profiles 64
- requirements 18, 64
- retry settings 149
- settings 67

McAfee
An Intel Company